Université de Montréal

La protection des données personnelles en droit international privé

Par
Justine Bertaud du Chazaud

Université de Montréal
Faculté de droit

Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître en droit
Maitrise en « Droit des technologies de l'information »

Décembre, 2015

Résumé

Les nouvelles technologies et l'arrivée de l'Internet ont considérablement facilité les échanges transnationaux de données entre les entreprises publiques et/ou privées et également entre les personnes elles-mêmes. Cependant cette révolution numérique n'a pas été sans conséquences sur l'utilisation de nos données personnelles puisque cette abondance de données à la portée de tiers peut conduire à des atteintes : la commercialisation des données personnelles sans le consentement de l'intéressé par des entreprises ou encore la diffusion de sa photographie, de son nom, de son prénom à son insu en sont des exemples.

La question qui vient alors se poser est en cas de litige, c'est-à-dire en cas d'atteintes au droit à la protection de nos données personnelles, présentant un ou des éléments d'extranéité, quels tribunaux pouvons-nous saisir ? Et quelle est la loi qui sera applicable ?

Les droits québécois, de l'Union européenne, et suisse présentent différents critères de rattachement intéressants et adaptés à des situations prenant place hors et sur internet. Le droit commun de chacun de ces systèmes est envisagé, puis appliqué aux données personnelles dans le cadre d'une situation normale, et ensuite à internet si la situation diffère. La doctrine est également analysée dans la mesure où certaines solutions sont tout à fait intéressantes, et cela notamment sur internet.

Un premier chapitre est consacré à la compétence internationale des tribunaux et aux critères de rattachement envisageables en droit commun à savoir notamment : le tribunal de l'État de survenance du préjudice, le tribunal de l'État de la faute ou encore le tribunal du domicile de la victime. Et ceux prévus ou non par la doctrine tels que l'accessibilité et le ciblage par exemple.

Les conflits de lois sont étudiés dans un deuxième chapitre avec également l'énumération les différents facteurs de rattachement envisageables en droit commun comme la loi de l'État du préjudice, la loi de l'État de la faute ou encore la loi de l'État favorisant la victime. Et également ceux prévus par la doctrine : la loi de l'État « *offrant la meilleure protection des*

données à caractère personnel »[1] ou encore la loi de l'État où est établi le « *maître du fichier* ».[2]

Le tribunal le plus compétent au regard des principes généraux de droit international privé en cas d'atteintes au droit de la protection des données personnelles hors et sur internet est le tribunal de l'État du domicile de la victime.

Et la meilleure loi applicable est la loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance, et dans le cas où la situation ne présente pas d'éléments d'extranéité, la meilleure loi est la loi favorisant la victime.

Mots-clés : Protection des données personnelles, Droit québécois, Droit européen, Droit suisse, Droit international privé, Atteintes, Droit à l'image, Flux transfrontaliers, Pourriel, Hameçonnage, Logiciel espion, Traceur, Compétence juridictionnelle, Conflits de lois, Préjudice, Faute, Domicile du défendeur/demandeur à l'instance, Ciblage, Accessibilité, Forum non conveniens, Émission, Réception, Localisation du serveur, Fournisseur d'accès à internet, Hébergeur, Intermédiaires, Maître du fichier, Facteurs et/ou Critères de rattachement, Solutions, Avantages et/ou Inconvénients, Internet.

[1] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[2] *Id.*

Summary

New technologies and the rising of the Internet boosted international data trade between public and/or private companies and even between individuals. However, this digital revolution is coming with its consequences: this exchange of data leads to personal data transactions (personal information or pictures for example) without users' will.

In case of violation of personal data, it is still unclear how to bring a case before the courts? Which Law is applicable?

Quebec Law, European Union Law and Swiss Legislation show similarities in real life and on the internet. First, we consider the common law, then personal data real life and on the Internet if there are any differences. The conceptual doctrine is also analysed as it reveals new Internet specific issues.

The first chapter tackles the international jurisdiction of the courts, potential criteria of ordinary law: the court where the damage occurs, the court where the conduct occurred or the court where the plaintiff lives; and those that are and are not covered by the doctrine as the accessibility and the targeting for example.

Law conflicts and multiple potential criteria of ordinary law are studied in the second chapter. The State of the damage, the State of the misconduct and the State that benefit to the victim among others. The regulation that ensures the best personal data protection and the law that identifies the file master.

From the international private law perspective, the most competent court is the one located in the State where the plaintiff is living when damage occurs. And the best regulation to follow is the he law of the country of domicile or the law of the law that promotes and protects the victim.

Keywords: Protection of personal privacy, Quebec Law, European Law, Swiss legislation, Private international law, Infringements, Use of personal image, Cross-border flaws, Spam, Phishing, Spyware, Tracker, Legal authority, Legal conflict, Damage, Fault, Domicile of the defendant/victim, Targeting, Accessibility, *Forum non conveniens* (literally, "inconvenient forum"), Uploading, Downloading, Server location, Internet Service provider, Host,

Intermediates, File master, Connecting factors, Solutions, Advantages and/or Disadvantages, Internet.

Tables des matières

Résumé ..... **i**

Summary ..... **iii**

Tables des matières ..... **v**

Liste des abréviations ..... **xi**

Remerciements ..... **xiii**

Introduction **1**

Chapitre préliminaire : Données personnelles et règles de droit international privé **5**

Section 1 : Définition de la notion de données personnelles **5**

A. Approche doctrinale et jurisprudentielle de la notion de données personnelles 5

1. Vie privée en tant que « *sous-ensemble* » des données personnelles 5

2. Données personnelles en tant que « *sous-ensemble* » de la vie privée 6

B. Données personnelles et encadrement législatif 9

Section 2. Atteintes au droit de la protection des données personnelles **14**

A. Flux transfrontaliers de données à caractère personnel 14

B. Autres atteintes au droit de la protection des données personnelles 19

C. Atteintes au droit de la protection des données personnelles et internet 22

1. Le « spamming », pourriel ou courrier indésirable 22

2. Le « *phishing* », hameçonnage ou courriel frauduleux 23

3. Le « *spyware* », logiciel espion ou mouchard 24

4. Le « *cookie* », témoin de connexion ou traceur 25

Section 3. Données personnelles et méthodes du droit international privé **27**

A. Données personnelles et détermination de la situation litigieuse 27

1. Données personnelles et statut personnel 28

2. Données personnelles et responsabilité civile contractuelle ou extracontractuelle 31

3. Données personnelles et lois de police 33

4. Sanctions 34

B. Données personnelles et objectifs des règles de droit international privé 35

1. Données personnelles et compétence juridictionnelle 35
2. Données personnelles et règles de conflits de lois 36
Synthèse 38

Chapitre 1 : Données personnelles et compétence internationale des tribunaux en droit québécois, européen et suisse 40

Section 1. Le tribunal du lieu du préjudice 42
A. Droit commun 42
B. Application aux données personnelles 44
Avantages et inconvénients 45
C. Situation sur internet 46
Avantages et inconvénients sur internet 47

Section 2. Le tribunal du lieu de la faute 48
A. Droit commun 48
B. Application aux données personnelles 49
Avantages et inconvénients 50
C. Situation sur internet 51
Avantages et inconvénients sur internet 51

Section 3. Le tribunal de l'État du domicile du défendeur 52
A. Droit commun 52
B. Application aux données personnelles 53
Avantages et inconvénients 53
C. Situation sur internet 54
Avantages et inconvénients sur internet 55

Section 4. Le tribunal de l'État du domicile de la victime 56
A. Droit commun 56
B. Application aux données personnelles 57
Avantages et inconvénients 57
C. Situation sur internet 57

Section 5. Le tribunal du centre principal des intérêts du demandeur 58
A. Solution spécifique 58
B. Application aux données personnelles 59
Avantages et inconvénients 59

Section 6. L'accessibilité 60

A. Présentation générale 60
B. Application aux données personnelles 63
Avantages et inconvénients 63
Section 7. Le ciblage 64
A. Présentation générale 64
B. Application aux données personnelles 66
Avantages et inconvénients 67
Section 8. Le tribunal de l'État de localisation du serveur informatique 67
A. Présentation générale 67
B. Application aux données personnelles 68
Avantages et inconvénients 68
Section 9. Le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires 69
A. Présentation générale 69
B. Application aux données personnelles 69
Avantages et inconvénients 70
Section 10. Le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige : le forum « *non conveniens* » 71
A. Droit commun 71
B. Application aux données personnelles 73
Avantages et inconvénients 76
C. Situation sur internet 76
Synthèse 78
Chapitre 2 : Données personnelles et conflits de lois 82
Section 1. La loi du lieu du préjudice 83
A. Droit commun 83
B. Application aux données personnelles 84
Avantages et inconvénients 85
C. Sur internet 85
Avantages et inconvénients sur internet 86
Section 2. La loi du lieu de la faute 88
A. Droit commun 88
B. Application aux données personnelles 88

Avantages et inconvénients ... 88
C. Sur internet ... 89
Avantages et inconvénients sur internet ... 90
Section 3. La loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance ... 92
A. Droit commun ... 92
B. Application aux données personnelles ... 93
Avantages et inconvénients ... 93
C. Sur internet ... 94
Section 4. La loi de l'État de la résidence habituelle du défendeur à l'instance ... 94
A. Droit commun ... 94
B. Application aux données personnelles ... 95
Avantages et inconvénients ... 95
C. Sur internet ... 96
Section 5. La loi de l'État favorisant la victime ... 97
A. Disposition particulière ... 97
B. Application aux données personnelles ... 97
Avantages et inconvénients ... 98
C. Sur internet ... 98
Section 6. L'accessibilité ... 99
A. Présentation générale ... 99
B. Application aux données personnelles ... 99
Avantages et inconvénients ... 100
Section 7. Le ciblage ... 100
A. Présentation générale ... 100
B. Application aux données personnelles ... 101
Avantages et inconvénients ... 102
Section 8. La loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires ... 103
A. Présentation générale ... 103
B. Application aux données personnelles ... 103
Avantages et inconvénients ... 104

Section 9. La loi de l'État « *offrant la meilleure protection des données à caractère personnel* » 105
A. Présentation générale 105
Avantages et inconvénients 106
B. Sur internet 107
Section 10. La loi de l'État où est établi le « *maître du fichier* » 107
A. Présentation générale 107
Avantages et inconvénients 108
B. Sur internet 108
Synthèse 109
Conclusion 112
Bibliographie 118

Liste des sigles

C.c.Q : Code civil du Québec.

CE : Conseil européen.

CEDH : Cour européenne des droits de l'Homme.

CJCE : Cour de Justice des Communautés européennes.

CJUE : Cour de Justice de l'Union européenne.

CNRS : Centre national de recherche scientifique.

Conv. ESDH : Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales.

CNIL : Commission nationale de l'informatique et des libertés.

FBI : Federal Bureau of Investigation

G.29 : Groupe des 29 Commissions nationales de l'informatique et des libertés.

IP : Internet Protocol.

NSA : National Security Agency

OCDE : Organisation de coopération et de développement économique.

TFUE : Traité sur le fonctionnement de l'Union européenne.

TGI : Tribunal de Grande Instance.

Liste des abréviations

Al. : Alinéa.

Art. : Article.

Ch. : Chambre

Etc. : Et cætera.

À ma famille, mes amis et particulièrement Chloé pour son soutien inconditionnel.

Remerciements

Je tiens à remercier Monsieur le Professeur Gérald Goldstein pour sa gentillesse, sa disponibilité, ses précieux conseils ainsi que pour sa maitrise indéniable du droit international privé,

Monsieur le Professeur Jérôme Huet, pour m'avoir enseigné avec tant de passion et ainsi transmis son attrait pour le droit des nouvelles technologies,

Monsieur le Professeur Vincent Gautrais, qui m'a conforté dans ma volonté de poursuivre dans cette voie juridique,

Mes parents, Pierre et Sylvie Bertaud du Chazaud, pour leur patience et encouragements,

Mon ami, Guillaume Rouby, pour m'avoir aidé à comprendre les outils informatiques et cela aux fins notamment, d'être plus à même d'appréhender le droit des nouvelles technologies,

D'autre part, il m'apparaît difficile de ne pas mentionner ici *Edward Snowden*, lanceur d'alertes américain, exilé aujourd'hui en Russie, qui a remis en exergue la nécessité qui incombe à chaque citoyen de protéger ses données personnelles et sa vie privée hors et sur internet.

Enfin, je tiens à saluer le travail effectué par Madame Laura Poitras, réalisatrice et journaliste d'investigation, pour son documentaire des plus audacieux, *Citizenfour,* retraçant l'affaire *Snowden,* et récompensé notamment lors de la 87ème cérémonie des Oscars en tant que meilleur film documentaire.

Introduction

« *Laura, à ce stade, je ne peux vous donner que ma parole. Je suis un fonctionnaire des renseignements américains. Vous contacter est extrêmement risqué. Pour le moment, sachez que tous vos voyages, tous vos achats, tous vos appels, toutes les antennes d'opérateur, tous vos amis, tout votre historique internet, tous vos articles sont entre les mains d'un système qui n'a pas de limites. Si vous publiez mes informations, je serais instantanément impliqué. Je vous demande de vous assurer que ces informations parviennent au peuple américain. Merci, soyez prudente. Citizenfour ».*[3]

Après le 11 septembre 2001, le Congrès américain a voté le *Patriot Act,*[4] une loi ayant pour objectif principal de solidifier les pouvoirs de l'*United States Intelligence Community* aux fins de lutter contre le terrorisme avec notamment la possibilité pour le FBI d' « *épier la circulation des messages électroniques et à conserver les traces de la navigation sur le Web de toute personne suspectée de contact avec une puissance étrangère ».*[5]

Toutefois, le récent scandale de l'affaire *Snowden* a mis en exergue les dérives liées à cette loi où l'agence de sécurité nationale américaine, la NSA, ainsi que ses partenaires internationaux (Royaume-Uni, Nouvelle-Zélande etc.) ont procédé à une surveillance mondiale d'internet et des autres moyens de communication.

La protection des données personnelles a donc pris une dimension tout autre avec l'affaire *Snowden.* Il semble y avoir eu une prise de conscience de la part des individus de la nécessité de protéger les données permettant de les identifier de la part des Gouvernements, mais également des entreprises privées qui n'hésitent pas à commercialiser celles-ci sans véritable consentement de la personne intéressée.

---

[3] POITRAS, L., « Citizenfour », *plateforme en ligne youtube.com* (2014), en ligne :
< https://www.youtube.com/watch?v=L8ygeb6F8ww > (consulté le 4 mai 2015).
[4] The Senate and The House of representatives of the United States of America, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, H.R. 3162, 107ème, 1ère session, 5 (2001), en ligne:
< http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf > (consulté le 11 février 2015).
[5] L'OBS Monde, « Qu'est-ce que le Patriot Act», *L'obs Monde* (6 septembre 2006), en ligne :
< http://tempsreel.nouvelobs.com/monde/20060906.OBS0822/qu-est-ce-que-le-patriot-act.html > (consulté le 29 avril 2015).

Les nouvelles technologies et notamment internet facilitent considérablement cet afflux massif de données personnelles. Que ce soit sur les réseaux sociaux (*Facebook*, *Twitter* etc.) ou encore sur les sites de vente en ligne dans lesquels nous communiquons des informations personnelles ou encore par de simples navigations sur internet où nous laissons des traces susceptibles de nous identifier ou plus exactement des traces susceptibles d'identifier notre genre masculin ou féminin, nos goûts, nos préférences etc. Il faut savoir que cela n'est pas sans conséquences et que nos données personnelles constituent une véritable « mine d'or » pour les entreprises.

Ainsi, avec un simple « *like* » ou « *j'aime* » sur le réseau social créé par Mark Zuckerberg par exemple, nous pouvons identifier le comportement d'un individu : il devient un « produit », un produit que *Facebook* commercialise alors aux autres entreprises.

Bien que la commercialisation de nos données soit antérieure à internet, elle semble avoir pris une toute autre ampleur depuis son avènement. Certes, l'utilisation des nouvelles technologies ont facilité les échanges de données personnelles, mais l'internaute a lui-même contribué à faciliter ces échanges en donnant ses données sans en avoir au préalable mesuré les conséquences.

La commercialisation de nos données sans ou avec notre consentement indirect, consentement indirect en ce sens qu'en s'inscrivant sur Facebook par exemple l'utilisateur consent à ne plus être maître de ses données, n'est pas le seul risque qui guette nos données personnelles. Nous pouvons penser aussi à un individu mal-attentionné qui choisit de diffuser des informations personnelles sans le consentement de l'intéressé tels que son nom, prénom et adresse postale et/ou courriel afin de lui nuire, ou qui cherche à récupérer ses numéros de cartes de crédit à des fins frauduleuses en se faisant passer pour un tiers, une institution financière par exemple.

C'est donc de l'ensemble de ces atteintes à nos données personnelles, et à notre droit de les protéger que nous allons aborder dans ce mémoire. Ce thème va être étudié sous la dimension du droit international privé : c'est-à-dire en cas de litige présentant un élément d'extranéité, entre des personnes physiques ou morales, quels sont les tribunaux que la victime de l'atteinte va pouvoir saisir, et quelle loi peut être applicable à ce litige.

Plusieurs critères de rattachement vont être envisageables, et il va être ici question de déterminer les meilleures solutions au regard des principes de droit international privé que nous allons évoquer, c'est-à-dire les solutions présentant le plus d'avantages possibles et le moins d'inconvénients pour la victime et de l'auteur du dommage.

L'étude de ce sujet se fera au regard du droit québécois, du droit de l'Union européenne et du droit français le cas échéant, c'est-à-dire notamment en matière de qualification juridique en ce qui concerne les atteintes aux données personnelles, et le droit suisse.

Le choix de ces trois systèmes juridiques est assez simple : il s'agit de législations variées et qui offrent certaines solutions en droit international privé des plus intéressantes et adaptées, notamment en ce qui concerne les atteintes au droit de la protection des données personnelles hors et sur internet.

Le droit suisse sera étudié car de nombreux États et/ou provinces se sont inspirés de son droit international privé. Le droit de l'Union européenne et le droit québécois seront également analysés car il s'agit de législations variées et offrant, on le verra, des solutions extrêmement intéressantes.

Nous allons donc envisager le droit commun de chacun de ces systèmes, c'est-à-dire quels critères de rattachement ils envisagent, l'appliquer aux données personnelles, puis à internet, si la situation diffère de la situation hors internet.

D'autre part, la doctrine va également être abordée puisqu'elle propose des solutions intéressantes qui méritent d'être analysées et appliquées aux données personnelles.

Il va donc être ici question de savoir quelle sera la meilleure juridiction pour connaitre d'un litige ayant trait à une atteinte au droit de la protection des données personnelles ? Et quelle sera la meilleure loi applicable en cas de litiges ? En d'autres termes, quelles sont les solutions les plus adaptées en cas de litiges internationaux en matière d'atteintes au droit de la protection des données personnelles ?

Dans un premier chapitre préliminaire, les données personnelles au regard des règles de droit international privé vont être abordées : nous allons nous attacher à définir la notion de

données personnelles d'après les législations québécoise, européenne et suisse et la doctrine, puis analyser les différentes atteintes au droit à la protection des données personnelles susceptibles de se matérialiser, et s'intéresser aux méthodes du droit international privé en matière de donnés personnelles, étape indispensable pour la suite de l'étude.

Dans le premier chapitre, nous allons étudier les données personnelles et la compétence internationale des tribunaux selon la législation québécoise, de l'Union européenne et suisse, et déterminer au regard des différentes solutions, quelle sera la meilleure, c'est-à-dire la plus adaptée dans le cas d'une atteinte au droit à la protection des données personnelles.

Et dans le deuxième chapitre, les données personnelles et les règles de conflits de lois, et à nouveau déterminer la loi présentant le plus d'avantages (et le moins d'inconvénients) à l'égard de la victime et de l'auteur d'une atteinte au droit de la protection des données personnelles. De la même façon, nous établirons la loi que nous considérons comme étant la meilleure la plus adaptée à un litige relatif à une violation des données personnelles.

D'autre part, à la fin de chaque chapitre (préliminaire, 1 et 2) une synthèse sera présentée et reprendra les points les plus importants qui ont été étudiés.

Dans le cadre de la conclusion, les différents éléments de chacune des synthèses seront repris afin de déterminer le ou les tribunaux le(s) plus compétent(s) ainsi que la ou les meilleure(s) loi(s) applicable(s) dans un litige en matière d'atteintes au droit de la protection des données personnelles.

Chapitre préliminaire : Données personnelles et règles de droit international privé

Dans le cadre de ce chapitre préliminaire, il s'agit avant tout de définir la notion de données personnelles afin de pouvoir délimiter le sujet (section 1), de s'intéresser aux atteintes associées au droit de la protection des données personnelles (section 2), puis aux méthodes du droit international privé en matière de données personnelles (section 3).

Section 1 : Définition de la notion de données personnelles

Les systèmes juridiques québécois et européen ont une conception différente des notions de données personnelles.

La différence d'appréciation est appuyée de manière générale par la doctrine et la jurisprudence (A.), ainsi que par la législation (B.) de chaque État, région pour l'Union européenne ou province pour le Québec.

A. Approche doctrinale et jurisprudentielle de la notion de données personnelles

L'Union européenne envisage la vie privée comme un « *sous ensemble* »[6] des données personnelles (1.). Cette conception n'est pas celle partagée au Québec où au contraire les données personnelles sont considérées comme un « *sous ensemble* »[7] de la vie privée (2).

1. Vie privée en tant que « *sous-ensemble* »[8] des données personnelles

Au sein de l'Union européenne, la notion de données personnelles a une portée beaucoup plus large que la notion du droit au respect de la vie privée : « *(...) les données personnelles englobent des éléments publics d'identification ou de connexion qui ne relèvent pas nécessairement de la vie privée, notamment l'état civil, les empreintes digitales ou*

[6] BENYEKHLEF, K., « Les normes internationales de protection des données personnelles et l'autoroute de l'information » dans *La vie privée dans l'entreprise*, éd. Thémis, Montréal, Actes des Journées Maximilien-Caron, 1996, p. 65.
[7] *Id.*
[8] *Id.*

génétiques, le numéro de sécurité sociale, les coordonnées bancaires ou l'adresse électronique ».[9]

L'Union européenne et les CNILS de chaque État membre (le G 29) ont émis une proposition de Règlement européen[10] dans laquelle elles se montrent « *favorables à l'élargissement de la notion de données personnelles à d'autres éléments susceptibles d'identifier indirectement les individus, et donc au-delà de leur vie privée : il s'agit notamment de l'adresse IP de l'ordinateur, des codes d'accès, des mots de passe ou de certains éléments comme le traçage des cookies (…), par géolocalisation, ou encore le traitement par croisement et classement de données publiques* ».[11]

Cette proposition formulée par l'Union européenne et les CNILS de chaque État membre parait très intrusive.

Autrement dit, selon la conception de l'Union européenne, les données personnelles doivent être perçues comme « englobant » la vie privée.

2. Données personnelles en tant que « *sous-ensemble* »[12] de la vie privée

Cette approche est celle qui prévaut en droit québécois. En effet, la doctrine québécoise considère que les données personnelles constituent un « *sous-ensemble* »[13] du droit à la vie privée.

À cet égard, l'auteur et Professeur à l'Université de Montréal, Monsieur Karim Benyekhlef, considère que : « *La variété des fonctionnalités de l'autoroute de l'information nous permet d'apprécier la diversité et l'inégale importance des possibles atteintes au droit à la vie privée. À ce propos, il convient de distinguer entre le droit à la vie privée et la protection des données*

[9] DUPUIS, M., « La vie privée à l'épreuve des réseaux sociaux », (2013) 102 *Revue Lamy Droit civil* 39.
[10] CE, *Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)* (2012).
[11] DUPUIS, M., « La vie privée à l'épreuve des réseaux sociaux », (2013) 102 *Revue Lamy Droit civil* 39.
[12] BENYEKHLEF, K., « Les normes internationales de protection des données personnelles et l'autoroute de l'information » dans *La vie privée dans l'entreprise*, éd. Thémis, Montréal, Actes des Journées Maximilien-Caron, 1996, p. 65.
[13] *Id.*

personnelles. La première notion englobe la seconde. Autrement dit, la protection des données personnelles n'est qu'un sous-ensemble du droit à la vie privée ».[14]

La doctrine québécoise semble avoir une conception large de la vie privée, et cela contrairement au droit européen où la doctrine accorde une place plus restreinte à la notion de vie privée en considérant qu'elle constitue un sous-ensemble des données personnelles.

La conception québécoise accorde donc une place plus importante à la personne qu'au sein des États membres de l'Union européenne.

Cette vision est aussi celle partagée par la Cour européenne des Droits de l'Homme. En effet, dans un arrêt K.U c. Finlande[15] la juridiction strasbourgeoise fait référence à la notion de vie privée et aucunement à celle de données personnelles.

En l'espèce, le requérant, mineur au moment des faits, avait été mentionné contre son gré dans une annonce de « sites de rencontres » sur internet. Celle-ci « *mentionnait son âge et son année de naissance et le décrivait physiquement de manière détaillée. Elle contenait également un lien vers sa page web où figuraient sa photographie et son numéro de téléphone, exact à un chiffre près ; et elle indiquait qu'il recherchait une relation intime avec un garçon de son âge ou plus âgé que lui (…)* ».[16]

Les juges ont estimé qu'il y avait une violation de la vie privée au regard de l'article 8 de la Convention européenne qui dispose : « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sureté publique, au bien-être économique du pays, à la défense de l'ordre et à la préservation des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».[17]

---

[14] BENYEKHLEF, K., « Les normes internationales de protection des données personnelles et l'autoroute de l'information » dans *La vie privée dans l'entreprise*, éd. Thémis, Montréal, Actes des Journées Maximilien-Caron, 1996, p. 65.
[15] *K.U c. Finlande,* n. 2872/02, CEDH 2008.
[16] *Id.*, &7.
[17] Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales,* 1950, en ligne : < http://conventions.coe.int/Treaty/FR/Treaties/Html/005.htm > (consulté le 14 février 2015).

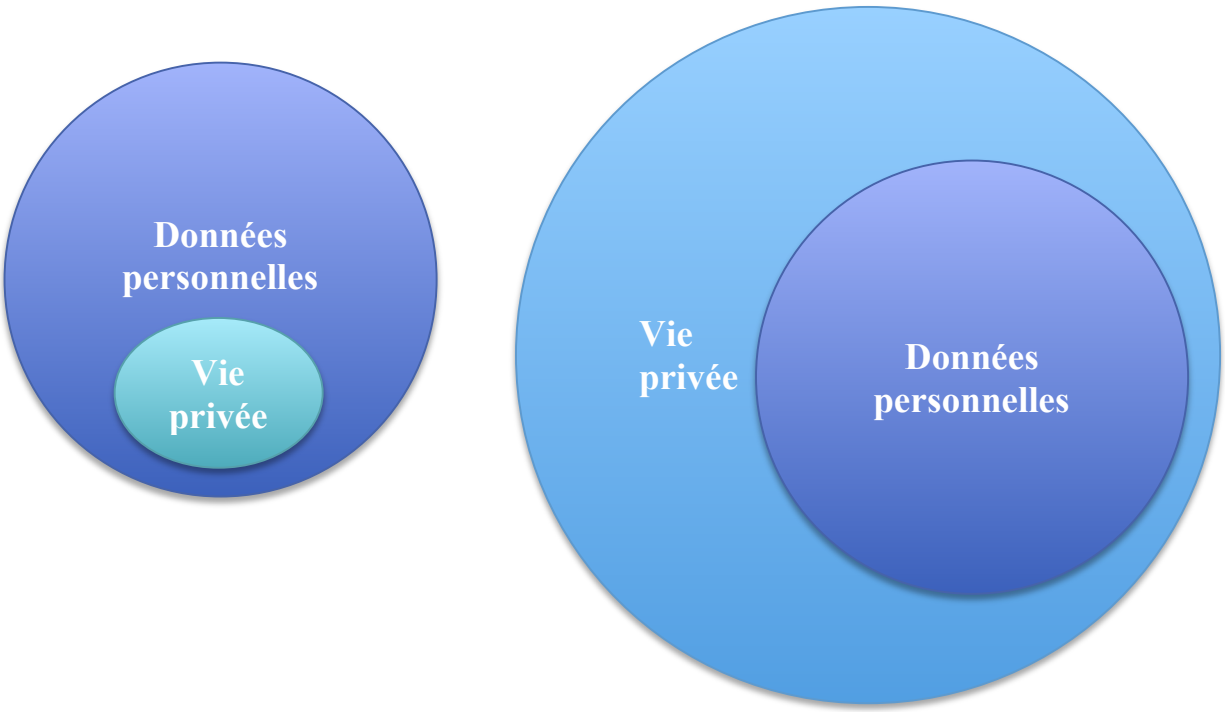
Ainsi, la Cour ne fait pas référence à la notion de données personnelles mais semble au contraire l' « englober » « *sous l'égide de l'article 8 de la Convention* ».[18]

Selon la doctrine québécoise et la jurisprudence du Conseil de l'Europe, la vie privée « englobe » la notion de données personnelles.

Finalement ce qui semble ressortir de ces deux approches ne concerne pas tant l'étendue des données personnelles, mais celui de la vie privée qui est différente selon les conceptions juridiques. Or, la vie privée ne rentre pas dans le champ de recherche du sujet.

Schéma

Union-européenne **Québec**



Au regard du schéma, on comprend bien que la taille du cercle concernant les données personnelles est constante pour les deux systèmes juridiques, ce qui n'est pas le cas de la vie

[18] DUPUIS, M., « La vie privée à l'épreuve des réseaux sociaux », (2013) 102 *Revue Lamy Droit civil* 39.

privée : le seul problème étant finalement l'étendue de la protection de la vie privée qui ne relève pas ici de l'étude du sujet.

Autrement dit, ce qui est large ou étroit selon les systèmes juridiques est le domaine de la vie privée mais pas la notion de données personnelles, qui elle reste constante.

Nous allons à présent étudier l'encadrement législatif ayant trait aux données personnelles (B.).

B. Données personnelles et encadrement législatif

Nous allons nous intéresser ici aux définitions apportées par les législations québécoise, européenne et suisse en matière de « donnée personnelle ».

En droit québécois, l'article 54 de *la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* définit la notion de « *renseignements personnels* » et considère que : « *dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier* ».[19]

Et l'article 1 de *la loi sur la protection des renseignements personnels dans le secteur privé* dispose que : « *La présente loi a pour objet d'établir l'exercice des droits conférés par les articles 35 à 40 du Code civil, en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil* ».[20]

Cette dernière disposition réfère donc la protection des renseignements personnels au Code civil Québécois.

Et l'article 2 de la même loi définit la notion de données personnelles : « *Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier* ».[21]

---

[19] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* L.R.Q., c. A-2.1, art.54.
[20] *Loi sur la protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39-1, art.1.
[21] *Id.,* art.2.

L'article 35 du Code civil québécois stipule que : « *Toute personne a droit au respect de sa réputation et de sa vie privée.*

Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise ».[22]

Selon le droit québécois, les données personnelles telles que définies par les différentes lois sont protégées par le Code civil sous la régie de la protection du droit au respect de la vie privée.

En droit européen, *la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*,[23] qui sera bientôt remplacée par le projet de Règlement européen de 2012[24] encore en discussion devant le Parlement européen, est un instrument juridique de l'Union européenne et « *s'applique aux données traitées par des moyens automatisés ainsi qu'aux données contenues ou appelées à figurer dans un fichier automatisé* ».[25]

À cet égard, « *les moyens automatisés* » peuvent être identifiés comme toutes données informatiques alors que les « *fichiers non automatisés* » correspondent à tout document papier, c'est-à-dire tout document non informatisé.

Il s'agit d'un texte de référence mettant en place un cadre règlementaire afin d'établir un niveau adéquat de protection des données personnelles des citoyens européens.[26]

L'article 2 a) de la directive 95/46/CE définit la notion de données personnelles : « <*données personnelles*> *: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un*

---

[22] *Code civil du Québec,* L.Q., 1991, c. 64. art. 35.
[23] CE, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR > (consulté le 15 février 2015).
[24] CE, *Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)* (2012).
[25] Europa, « Protection des données à caractère personnel », (1 février 2011), en ligne :
< http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm > (consulté le 5 février 2015).
[26] *Id.*

u plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».[27]

L'article 2 a) du *Règlement européen 45/2001/CE relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données* dispose que : « *<données à caractère personnel> : toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».*[28]

L'Union européenne a adopté *la directive 2002/58/CE relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*[29] afin de protéger la vie privée des citoyens européens sur internet et a pour principale vocation de s'intéresser aux aspects délaissés par la directive de 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.[30] En effet, la directive 2002/58/CE élargit le champ d'application de la directive 95/46/CE en matière de données personnelles sur internet. À cet égard, le présent texte énumère successivement la nécessité et l'obligation pour les États membres de l'Union européenne de garantir la « *sécurité du traitement* », la « *confidentialité des communications* », la « *rétention des données* », les « *communications*

---

[27] CE, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR > (consulté le 15 février 2015).

[28] CE, *Règlement européen n.45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,* 2001, en ligne :
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF> (consulté le 7 février 2015).

[29] CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),* 2002, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR > (consulté le 7 février 2015).

[30] CE, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR > (consulté le 15 février 2015).

non sollicitées » ou « *spamming* », les « *témoins de connexion* » plus connus sous le nom de « *cookies* ».[31]

L'article 2 de la directive dispose que : « *Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre règlementaire commun pour les réseaux et les services de communications électroniques (directive « cadre ») s'appliquent aux fins de la directive ».*[32]

Il faut ici retenir que le droit de l'Union européenne définit la notion de données personnelles à travers les directives et son règlement. Toutefois, les données personnelles sont protégées par le droit interne de chaque État membre. À cet égard, l'article 9 du Code civil français dispose que : « *Chacun a droit au respect de sa vie privée* ».[33] Nous pouvons donc penser que de la même façon qu'en droit québécois, les données personnelles sont protégées par le Code civil sous la régie de la protection du droit au respect de la vie privée.

En droit suisse, l'article 13 de la Constitution fédérale de la Confédération suisse relatif à la protection de la sphère privée dispose que : « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.*

2. Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent ».[34]

Et l'article 3 de la loi sur la protection des données définit la notion de données personnelles : « *a. données personnelles (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable ;*

---

[31] Europe, « Protection des données dans le secteur électronique », (19 mai 2010), en ligne : < http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_fr.htm > (consulté le 2 avril 2015).
[32] CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),* 2002, en ligne : < http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR > (consulté le 7 février 2015).
[33] *Code civil,* art.9.
[34] *Constitution fédérale de la Confédération suisse*, 18 avril 1999, 101, art.13.

c. données sensibles, les données personnelles sur : 1. Les opinions ou activités religieuses, philosophiques, politiques ou syndicales,

2. la santé, la sphère intime ou l'appartenance à une race,

3. des mesures d'aide sociale,

4. des poursuites ou sanctions pénales et administratives ».[35]

En droit suisse, les données personnelles sont définies par la loi fédérale sur la protection des données et protégées par la Constitution suisse sous la régie du droit au respect de la vie privée.

Nous pouvons retenir plusieurs points importants dans cette première section.

Tout d'abord, le domaine des données personnelles reste constant et que ce qui est large ou étroit selon les systèmes juridiques étudiés est l'étendue de la vie privée. Or la vie privée ne fait pas partie du sujet.

Au regard des différentes législations et de la doctrine citées, nous pouvons définir les données personnelles comme étant des éléments permettant d'identifier un individu directement tels que le nom, le prénom, une photographie mais également d'identifier un individu indirectement avec l'adresse IP, le numéro d'assurance sociale, le lieu et la date de naissance etc.

Les données personnelles se distinguent donc de la diffamation qui est le fait de tenir des propos portant atteinte à l'honneur et à la réputation d'une personne, ce qui est différent.

Autrement dit, il ne sera donc pas question ici d'aborder le thème de la vie privée ou encore de la diffamation mais seulement des données personnelles au regard de la définition précitée.

Concernant l'encadrement législatif des données personnelles, nous remarquons qu'en droit québécois, les lois sur la protection des renseignements personnels dans le domaine public et privé définissent cette notion, mais c'est le Code civil québécois qui encadre la protection des données sous la régie du droit au respect de la privée.

---

[35] *Loi fédérale sur la protection des données*, 19 juin 1992, 235.1, art.3.

En droit européen, ce sont les directives 95/46/CE et 2002/58/CE ainsi que le Règlement 45/2001/CE qui définissent la notion de données. Cependant s'agissant de la protection des données, celle-ci est encadrée par la législation interne de chaque État membre de l'Union européenne.

Et en droit suisse, c'est la loi fédérale sur la protection des données qui définit la notion, et la Constitution suisse qui la protège sous la régie du droit au respect de la vie privée.

À présent, nous allons nous intéresser aux atteintes au droit de la protection des données personnelles (section 2). L'intérêt de cette section est ici de comprendre comment se matérialisent ces atteintes. Cette partie est importante puisqu'elle va permettre de visualiser les éléments susceptibles de caractériser une atteinte au droit de la protection des données personnelles et donc un litige.

Section 2. Atteintes au droit de la protection des données personnelles

Une atteinte aux données personnelles peut être matérialisée par le biais des flux transfrontaliers entre entreprises (A.), mais plus généralement par la divulgation de tous éléments permettant d'identifier un individu (B.). D'autre part, certaines atteintes au droit de la protection des données personnelles prennent place uniquement sur internet (C.).

A. Flux transfrontaliers de données à caractère personnel

Les flux transfrontaliers de données à caractère personnel s'apparentent à une transmission de données à caractère personnel qui est effectuée d'un État vers un autre État membre de la même organisation (par exemple l'Union européenne) ou vers un État tiers (dans le cas de l'Union européenne, cela signifie un État extérieur à l'Union européenne).[36]

Les flux transfrontaliers de données à caractère personnel peuvent être le fait d'organismes privés, c'est-à-dire des entreprises d'envergure internationale qui échangent des informations

[36] Commission de la protection de la vie privée, « Questions les plus fréquemment posées - Flux transfrontières de données à caractère personnel », *privacycommission,* en ligne :
< http://www.privacycommission.be/fr/faq-page/374#t374n7382 > (consulté le 2 avril 2015).

personnelles concernant des individus, ou à contrario, le fait d'organismes publics en ne respectant pas la législation de l'un ou l'autre État.

À cet égard, il convient de préciser qu'il n'existe pas d'harmonisation de la protection des données personnelles au niveau international, et cela peut donc avoir pour effet qu'une atteinte aux flux transfrontaliers peut être caractérisée dans un État, mais pas nécessairement dans un autre. En effet, les atteintes découlant de cette communication des données personnelles des individus entre les organismes sont principalement dues au fait que les législations en la matière diffèrent entre les États : certains systèmes législatifs ayant une conception plus « stricte » que d'autres en matière de flux transfrontaliers. Or le non-respect d'une norme législative par une entreprise peut entrainer une atteinte au droit à la protection des données personnelles.

Les atteintes sont donc la plupart du temps le fait d'un échange de données personnelles à l'extérieur d'un l'État, d'une province (Québec) ou encore d'un espace commun (Union-européenne).

Au niveau international, l'OCDE, une organisation internationale regroupant les pays « développés » a émis au début des années 80 des lignes directrices sur la protection de la vie privée et les flux transfrontaliers de données à caractère personnel[37] afin d'encadrer la vie privée et les flux transfrontières de données personnelles. Ces mêmes lignes ont par la suite été modifiées afin de faire face aux nouveaux défis lancés par internet. Il s'agit cependant de recommandations qui n'ont pas d'effets juridiques contraignants.

Au niveau provincial, régional ou national, le droit québécois, le droit de l'Union européenne et le droit suisse ont encadré les flux transfrontaliers de données à caractère personnel.

---

[37] *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* OCDE,1980, en ligne : <http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaractereperson nel.htm > (consulté le 10 février 2015).

Au Québec, la loi sur la protection des renseignements personnels dans le secteur privé[38] établit « *des règles à l'égard de la collecte, de l'utilisation et de la communication des renseignements personnels recueillis par une entreprise ou un ordre professionnel à des fins commerciales dans la province ».*[39]

L'article 17 de cette même loi stipule que : « *La personne qui exploite une entreprise au Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer : 2. (...) Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1. Et 2., elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte ».*[40]

Eu égard à cette disposition, il semble qu'un organisme privé, c'est-à-dire une entreprise souhaitant communiquer à un tiers qui se trouve à l'extérieur du Québec, une information relative à un individu, doit s'assurer de respecter deux éléments : « *Premièrement, elle doit s'assurer que ces renseignements ne seront pas utilisés, sans le consentement des personnes concernées, à d'autres fins que celles pour lesquelles ils ont été recueillis, sauf dans quelques cas d'exception stipulés dans la loi, notamment en matière criminelle. Deuxièmement, elle doit accorder aux personnes concernées la possibilité de retirer leurs renseignements nominatifs d'une liste si cette dernière est utilisée à des fins de recherche commerciale ou philanthropique ».*[41]

Autrement dit, une atteinte aux flux transfrontaliers de données à caractère personnel sera constituée selon le droit québécois dès que l'entreprise privée n'a pas recueilli le consentement de la personne intéressée, et également l'impossibilité pour l'intéressé de retirer ses informations personnelles d'une liste à caractère commerciale.

---

[38] *Loi sur la protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39-1.
[39] TREMBLAY, M., « Flux transfrontalières de données et protection de la vie privée », (2010) vol. III *Cahier de recherche.*
[40] *Loi sur la protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1., art. 17.
[41] TREMBLAY, M., « Flux transfrontalières de données et protection de la vie privée », (2010) vol. III *Cahier de recherche.*

Au sein de l'Union européenne, la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[42] est un instrument juridique de l'Union européenne et « *s'applique aux données traitées par des moyens automatisés ainsi qu'aux données contenues ou appelées à figurer dans un fichier automatisé* ».[43]

L'Union européenne avait par exemple mis en place des règles de *Safe Harbour* à destination des États-Unis et d'autres États qui étaient : « *un ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établis aux États-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne* ».[44] Cependant, ces règles ont été invalidées par la Cour de Justice de l'Union européenne le 6 octobre 2015.[45]

L'article 25 de la directive[46] énonce le cas des transferts de données personnelles à l'extérieur de l'Union européenne. À cet égard, un État européen qui opère vers un État tiers, un transfert de données à caractère personnel, doit s'être assuré au préalable que le pays « *récepteur* » de ces informations « *assure un niveau de protection adéquate* ».[47] Ainsi, l'absence d'une « *protection adéquate* »[48] entraine une atteinte aux données personnelles.

D'autre part, l'article 8 de la Charte des droits fondamentaux de l'Union européenne stipule que : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et*

---

[42] CE, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR > (consulté le 15 février 2015).
[43] Europa, « Protection des données à caractère personnel », (1 février 2011), en ligne :
< http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm > (consulté le 5 février 2015).
[44] Commission Nationale de l'Informatique et des Libertés, « Safe Harbour », en ligne :
< http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/safe-harbor/ > (consulté le 23 septembre 2015).
[45] *Maximillian Schrems c. Data Protection Commissioner,* Affaire C-362/14, 6 octobre 2015, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=50254 >, (consulté le 20 octobre 2015);
[46] Conseil européen, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR > (consulté le 15 février 2015).
[47] *Id.*
[48] *Id.*

d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».[49]

Ainsi, au regard de la Charte des droits fondamentaux, l'absence de loyauté dans le traitement des données ainsi que le non-consentement de l'intéressé sont susceptibles de constituer une atteinte aux données personnelles.

Les échanges de données personnelles entre entreprises établies au sein de l'Union européenne ne posent pas de difficultés. Toutefois, dans le cas de transferts hors Union européenne, l'État tiers doit assurer une protection adéquate c'est-à-dire équivalent au niveau de protection établi au sein de l'Union européenne : un niveau non adéquat entrainera alors une atteinte au droit à la protection des données personnelles par le biais des flux transfrontaliers.

En droit suisse, l'article 4 de la loi fédérale sur la protection des données dispose que : *« 1. Tout traitement de données doit être licite. 2. Leur traitement doit être effectué conformément aux principes de la bonne foi et de la proportionnalité. 3. Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. 4. La collecte de données, et en particulier les finalités du traitement doivent être reconnaissables pour la personne concernée. 5. Lorsque son consentement est requis pour justifier le traitement de données personnelles la concernant, la personne concernée ne consent valablement que si elle exprime sa volonté librement et après avoir été dûment informée. Lorsqu'il s'agit de données sensibles et de profils de la personnalité, son consentement doit être au surplus explicite ».*[50]

L'article 6 de la même loi concernant les « communications transfrontières » stipule qu' « *aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat ».*[51]

---

[49] CE, *Charte des droits fondamentaux de l'Union européenne,* 2000, en ligne :
< http://www.europarl.europa.eu/charter/pdf/text_fr.pdf > (consulté le 13 février 2015).
[50] *Loi fédérale sur la protection des données*, 19 juin 1992, 235.1, art. 4.
[51] *Id.,* art.6.

Autrement dit, le traitement de données personnelles ne doit pas être détourné de son objectif principal, et dans certains cas, le consentement de la personne intéressée est requis. S'agissant des flux transfrontaliers, de la même manière qu'en droit de l'Union européenne, l'absence de protection adéquate des données personnelles, c'est-à-dire un niveau de protection équivalent au droit suisse tel que mentionné par l'article 6 de la loi,[52] dans le cadre d'un transfert à l'étranger, entraine une atteinte au droit de la protection des données personnelles.

Nous avons donc vu ici qu'une atteinte au droit de la protection des données personnelles pouvait être constituée par le biais des flux transfrontaliers. Nous allons nous intéresser à présent aux autres atteintes au droit de la protection des données personnelles (B.).

B. Autres atteintes au droit de la protection des données personnelles

Dans le cadre de ce développement, il s'agit de s'intéresser aux autres cas d'atteintes au droit de la protection des données personnelles, à savoir l'utilisation d'une photographie, la divulgation d'éléments permettant d'identifier une personne par un tiers. Dans un rapport à l'attention du Conseil de l'Europe, Monsieur Jean Philippe Walter met en avant différents exemples d'atteintes au droit de la protection des données personnelles, autres que par le biais des flux transfrontaliers :

« Un collège ou une association sportive publie sur Internet, sans mauvaise intention et souvent par ignorance, des photos d'enfants ou de jeunes adultes avec le nom, voire l'adresse. Des jeunes participent à des forums de discussion et publient avec forces détails des informations les concernant qui par quelques clics sont accessibles de n'importe quel coin de la planète. Une agence hungaro-américaine proposait sur son site Internet des enfants hongrois en vue d'adoption à l'étranger. Sur le site figurait la photo, la date de naissance et les maladies éventuelles ».[53]

Nous pouvons également citer le cas de l'affaire *Ashley Madison*, un site de rencontre canadien dédié aux aventures « extraconjugales », où un groupe de pirates informatiques

[52] *Loi fédérale sur la protection des données*, 19 juin 1992, 235.1, art.6.
[53] WALTER, J-P., Conseil de l'Europe, *Défis posés par les flux transfrontières de données à caractère personnel,* Madrid, p.2.

avaient réussi à infiltrer le réseau interne de l'entreprise et ont divulgué des données personnelles des membres du site sur internet (photographies, courriels, numéro de carte bancaire etc.).

Nous allons ici donner quelques exemples susceptibles de constituer des atteintes aux données personnelles en droit québécois, en droit européen et en droit suisse.

En droit québécois, l'article 36 du Code civil énumère les différentes atteintes à la vie privée : « *Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :*

1° Pénétrer chez elle ou y prendre quoi que ce soit ;

2° Intercepter ou utiliser volontairement une communication privée ;

3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés ;

4° Surveiller sa vie privée par quelque moyen que ce soit ;

5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public ;

6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels ».[54]

Le droit québécois énumère donc successivement l'ensemble des faits susceptibles de constituer une atteinte aux données personnelles.

En droit européen, le nouvel alinéa 1 de l'article 16 du Traité sur le Fonctionnement de l'Union européenne dispose que : « *Toute personne a droit à la protection des données à caractère personnel la concernant ».*[55]

Le droit de l'Union européenne ne donne pas d'exemples sur ce qui est susceptible de constituer ou non une atteinte aux données personnelles contrairement au droit québécois. C'est la législation et la jurisprudence des États membres qui permettent de connaitre les différents faits susceptibles de constituer une atteinte ou non aux données personnelles

---

[54] *Code civil du Québec,* L.Q., 1991, c. 64., art.36.
[55] CE, *Traité sur le fonctionnement de l'Union européenne (version consolidée),* 2012, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012E/TXT&from=FR > (consulté le 5 février 2015).

En droit suisse, l'article 13 de la Constitution,[56] préalablement cité, ne donne pas des exemples permettant de considérer que tel ou tel fait constitue une atteinte aux données personnelles.

Ainsi, le droit suisse de la même manière que le droit de l'Union européenne, et à la différence du droit québécois, n'énumère pas les faits susceptibles de constituer une atteinte aux données personnelles.

Chaque État ne partage pas nécessairement la même vision de ce qui est susceptible de constituer une atteinte ou non aux données personnelles.

Pour illustrer ce propos, c'est-à-dire la vision divergente des États en matière de constitution d'atteintes aux données personnelles, prenons l'affaire Maria Pia Grillo c. Google Inc. :[57] prenant place au Québec. En l'espèce, la requérante a été photographiée par une voiture de « *Google Street View* » devant le porche de sa maison. À cet égard, une des questions à laquelle la Cour du Québec devait répondre était celle de savoir si la requérante se trouvait « *dans un endroit privé ou public lorsque son image a été captée ? ».*[58] La Cour n'a pas accepté « *la thèse selon laquelle la demanderesse, parce qu'elle était assise sur une marche extérieure de sa maison, et donc qu'elle était visible de la rue publique, avait nécessairement ou tacitement, de ce seul fait, renoncé à la protection de sa vie privée et de son image ».*[59]

La juridiction québécoise considère ici qu'il y a une atteinte au droit à l'image dans la mesure où la requérante se trouvait dans un endroit privé, à savoir devant le porche de sa maison. Or, une telle conception ne serait pas nécessairement partagée par d'autres juridictions étrangères qui au contraire, auraient eu tendance à considérer que la demanderesse en l'espèce se trouvait dans un lieu public.

D'après les exemples énoncés notamment par le droit québécois, les atteintes aux données personnelles autres que par le biais des flux transfrontaliers sont assez variées : cela

---

[56] *Constitution fédérale de la Confédération suisse*, 18 avril 1999, 101, art.13.
[57] *Maria Pia Grillo c. Google inc.*, C.Q. Montréal (Ch. Civ.), n. 500-32-130991-112, 3 octobre 2014, en ligne : < http://fr.scribd.com/doc/244927017/Google-Street-View-Case#scribd > (consulté le 3 mars 2015).
[58] *Id.,* &44.
[59] *Id.,* &51.

peut être une atteinte au droit à l'image ou la diffusion du nom d'une personne ou la diffusion finalement de tous les éléments permettant l'identification d'un individu etc.

Les atteintes aux données personnelles ont été multipliées avec le numérique, et cela notamment par le biais des réseaux sociaux.[60] Certaines atteintes sont antérieures à l'avènement d'internet, par exemple les atteintes au droit à l'image, ou encore les atteintes par le biais des flux transfrontaliers et ont été facilitées avec internet, mais d'autres sont nées avec l'arrivée d'internet, et ce sont ces atteintes que nous allons étudier : les atteintes au droit de la protection des données personnelles et internet (C.).

C. Atteintes au droit de la protection des données personnelles et internet

L'intérêt de cette section est d'établir les différentes atteintes aux données personnelles prenant place uniquement sur internet : le « *spamming* », pourriel ou courrier indésirable (1.), le « *phishing* », hameçonnage ou courriel frauduleux (2.), le « *spyware* », logiciel espion ou mouchard (3.), et enfin le « *cookie* », témoin de connexion ou traceur (4.).

1. Le « spamming », pourriel ou courrier indésirable

Le « *spamming* », pourriel ou courrier indésirable consiste en « *l'envoi massif et répété de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'internet : forums de discussion, listes de diffusion, annuaires, sites web, etc. ».*[61]

Ce type de pratiques est, en règle générale, contraire aux législations en vigueur en matière de protection des données personnelles. En effet, un rapport de la CNIL française met en avant le fait que l'adresse électronique d'un individu est considérée comme une donnée personnelle : « *(...) une adresse électronique d'un individu est évidemment une information nominative : directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse ; en*

---

[60] LAMBERT-CHAN, M., «Les médias sociaux décuplent les poursuites pour diffamation», *UdeMNouvelles*, 9 mai 2011, en ligne : <http://www.nouvelles.umontreal.ca/recherche/sciences-sociales-psychologie/20110509-les-medias-sociaux-decuplent-les-poursuites-pour-diffamation.html > (consulté le 2 novembre 2014).

[61] ALVERGNAT, C., CNIL, *Rapport sur le publipostage électronique et la protection des données personnelles*, Paris, 1999, en ligne : < http://www.diocese-alsace.fr/docs/juridiques/loi-cnil-publipostage.pdf > (consulté le 8 janvier 2015).

tout état de cause, toujours indirectement nominative dans la mesure où toute adresse électronique est associée à un nom et à une adresse physique (…) ».[62]

La CNIL précise qu' « *Il s'agit tout d'abord de déterminer les conditions dans lesquelles des données personnelles (ici, l'email) peuvent être collectées et utilisées à des fins de prospection ; il s'agit, ensuite, d'apprécier les garanties qui doivent être mises en œuvre pour permettre aux personnes, le cas échéant, de s'opposer à faire l'objet de prospections ».*[63]

Il y a une obligation de requérir, avant l'envoi de tout courriel publicitaire, le consentement préalable du principal intéressé, est nécessaire. Autrement dit, l'absence de ce consentement constitue une atteinte à la protection des données personnelles.

Autrement dit, le fait d'intercepter une adresse courriel par le biais des réseaux publics ou par tout autre moyen afin d'envoyer des courriels commerciaux sans le consentement de l'intéressé constitue une atteinte aux données personnelles.

2. Le « *phishing* », hameçonnage ou courriel frauduleux

Le « *spamming* », pourriel ou courriel indésirable se distingue du « *phishing* », hameçonnage ou courriel frauduleux. En effet, le « *pourriel ne conduit pas toujours à l'hameçonnage mais de plus en plus, il est un vecteur pour faciliter la commission de gestes illicites ».*[64]

Le « *phishing* » consiste en « *l'envoi, par des criminels, de courriels, de messages textes et de sites web qui sont conçus pour avoir l'air de provenir d'entreprises, d'institutions financières et d'organismes gouvernementaux légitimes bien connus et qui visent à tromper le destinataire*

---

[62] ALVERGNAT, C., CNIL, *Rapport sur le publipostage électronique et la protection des données personnelles*, Paris, 1999, en ligne : < http://www.diocese-alsace.fr/docs/juridiques/loi-cnil-publipostage.pdf > (consulté le 8 janvier 2015).
[63] *Id.,* p.2.
[64] TRUDEL, P., AUBRAN, F., DUPUIS, G., Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Montréal, 2007, p.7.

afin de lui soutirer des renseignements personnels, financiers ou de nature délicate ».[65] Ce type de pratique peut « *faciliter l'usurpation d'identité* ».[66]

Le fait de se faire passer pour une entreprise publique ou privée afin de soutirer des renseignements personnels est constitutif d'une atteinte aux données personnelles.

3. Le « *spyware* », logiciel espion ou mouchard

Ce type de pratique ayant pour objectif principal de « récolter » des informations sur un internaute afin de « *les transmettre à des tiers* », « *et ce, sans avoir obtenu au préalable son véritable consentement* ».[67] En règle générale, les logiciels espions « *sont réalisés à partir d'éléments que l'on télécharge sur le Web »*[68], et qui « *ne sont pas détectables par l'internaute* ».[69] Cette pratique porte atteinte aux données personnelles et à la vie privée des internautes dans la mesure où « *un logiciel espion est généralement employé pour effectuer du cybermarketing « agressif » et – dans de plus rares cas – prendre possession de renseignements personnels pour réaliser des activités illicites ».*[70]

À certains égards, l'utilisation de logiciels espions a pour principal objectif l'aspiration d'adresses électroniques afin d'adresser aux internautes des courriels non-sollicités, c'est-à-dire des « *spams* ». Dans un arrêt du 14 mars 2006, la Chambre criminelle de la Cour de cassation française[71] a considéré que l'utilisation de « *logiciels permettant d'aspirer sur des espaces accessibles au public d'internet (forums de discussion, sites…) des adresses électroniques de personnes physiques afin de leur adresser des courriels publicitaires non sollicités (ou spams) »*[72] était illégale.

---

[65] Gendarmerie Royal du Canada, « Courriels frauduleux et hameçonnage (phishing) », (29 janvier 2015), en ligne : < http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-fra.htm > (consulté le 10 février 2015).
[66] TRUDEL, P., AUBRAN, F., DUPUIS, G., Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Montréal, 2007, p.13.
[67] *Id.*, p.23.
[68] Dictionnaire de la High Tech, « Spyware logiciel espion », en ligne : < http://encyclopedie.linternaute.com/definition/491/5/spyware.shtml > (consulté le 10 février 2015).
[69] *Id.*
[70] TRUDEL, P., AUBRAN, F., DUPUIS, G., Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Montréal, 2007, p.23.
[71] Crim. 14 mars 2006, *Bull. crim.,* n.69.
[72] HUET, J., DREYER, E., *Droit de la communication numérique,* coll. "Manuel", Paris, éd. LG.D.J Lextenso, 2011, p.328.

L'intrusion dans le système informatique d'autrui par le biais d'un logiciel destiné à intercepter des renseignements personnels tels que les adresses courriels ou toute autre information constitue une atteinte aux données personnelles.

4. Le « *cookie* », témoin de connexion ou traceur

Il s'agit de fichiers « *déposés et lus par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé tels qu'un ordinateur un Smartphone, une liseuse numérique et une console de jeux vidéo connectés à Internet* ».[73]

Toutefois, ce type de pratiques porte-il réellement atteinte aux données personnelles de l'internaute ? Cette problématique vient à se poser dans la mesure où le traçage du comportement d'un utilisateur par le biais de fichiers permet la collecte d'une masse importante de données à caractère privé et/ou personnel, et cela sans le consentement du principal intéressé.

La doctrine française et européenne de manière plus générale considère que le traitement d'une donnée personnelle ou tout autre forme de traçage ne relève pas nécessairement du domaine des données personnelles[74] puisqu'il « *est vrai que ce qui fait l'objet de toutes les attentions des professionnels du numérique sur les réseaux sociaux est moins la vie privée des individus que le traçage de leur comportement, ce qui, pour une juridiction civile, reste en dehors du respect de la vie privée* ».[75] Dès lors, le traçage du comportement des internautes ne semble pas constituer une atteinte directe aux données personnelles.

Cette appréciation doctrinale française et européenne peut être remise en cause. À cet égard, il parait possible de considérer que le traçage d'un individu par le biais des « *cookies* » porte atteinte au respect de sa vie privée et de ses données personnelles dans la mesure où la navigation sur internet peut revêtir un aspect personnel. En effet, le fait de suivre un internaute

---

[73] Commission nationale de l'informatique et des libertés, « Cookies & traceurs : que dit la loi ? », *CNIL*, en ligne : < http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/ > (consulté le 14 février 2015).
[74] DUPUIS, M., « La vie privée à l'épreuve des réseaux sociaux », (2013) 102 *Revue Lamy Droit civil* 39.
[75] *Id.*

à chacune de ses connexions afin par la suite de le diriger ou l'orienter vers d'autres sites ou mettre en place une publicité ciblée eu égard à sa navigation, revient finalement à une violation de ses données personnelles.

Le fait de suivre ou « tracer » un internaute par le biais d'un cookie afin d'analyser ses goûts et ses préférences afin de lui proposer par le biais de publicités ciblées des produits susceptibles de l'intéresser pourrait être constitutif d'une atteinte aux données personnelles.

Ainsi les atteintes prenant place uniquement sur internet ont un but exclusivement commercial : recueillir les informations de l'internaute et notamment son adresse courriel, suivre ses goûts et préférences afin de pouvoir envoyer de la publicité de manière ciblée ou non. Il n'y a finalement que le « *phishing* » qui n'a pas nécessairement un caractère commercial mais est une pratique visant surtout à escroquer l'internaute ou à usurper son identité.

De manière générale, les atteintes aux données personnelles prenant place hors et sur ou uniquement sur internet sont relativement variées dans la mesure où l'atteinte peut avoir un caractère commercial, une intention de nuire à autrui par la diffusion d'une photographie ou de tout élément permettant l'identification d'un individu ou encore un caractère frauduleux avec l'usurpation d'identité ou la fraude à la carte bancaire notamment.

Après avoir défini la notion de données personnelles au regard du droit québécois, de l'Union européenne et suisse et identifié les différentes atteintes au droit de la protection des données personnelles susceptibles de prendre hors et/ou sur internet, nous allons nous intéresser aux méthodes du droit international privé afin de pouvoir ensuite aborder le thème principal du sujet (section 3).

Section 3. Données personnelles et méthodes du droit international privé

Dans le cadre de cette section, il s'agit d'étudier la détermination des situations litigieuses (A.), puis les facteurs de rattachement (B.) relatifs aux données personnelles.

A. Données personnelles et détermination de la situation litigieuse

Dans le cadre d'un litige international, c'est-à-dire un litige comprenant un ou plusieurs éléments d'extranéité, « *il faut préalablement effectuer un choix entre les règles de droit international privé : parmi les règles de conflit en présence, quelle est celle qui désignera l'ordre juridique compétent ? ».*[76] Ainsi, « *la méthode qu'il convient d'employer consiste à qualifier la question posée, c'est-à-dire à la classer dans l'une ou l'autre des catégories définies par les règles de conflit en présence, sélectionnant par-là celle qui doit être appliquée ».*[77]

Autrement dit : « *Si l'on admet qu'une règle substantielle doit être appliquée à la question de droit, la première façon de la choisir parmi les lois en présence consiste à s'interroger sur la nature de la question de droit et à en déduire quel élément la localise, c'est-à-dire détermine l'ordre juridique avec lequel elle présente objectivement les liens les plus significatifs ».*[78]

Avant de poursuivre, il faut préciser que les problèmes en matière de qualification peuvent également concerne la compétence juridictionnelle et pas seulement les conflits de lois. D'autre part, la qualification donnée dans le cadre de la compétence juridictionnelle ne sera pas forcément la même qualification donnée dans le cadre du conflit de lois. En d'autres termes : « *tandis que pour le conflit de lois ce dernier doit tenir compte de l'adéquation des catégories avec le critère de rattachement qui lui est associé, en matière de compétence*

---

[76] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.124.
[77] *Id.*
[78] *Id.,* p.94.

juridictionnelle son choix doit être dicté par la recherche du juge le mieux placé pour connaitre du différend ».[79]

Nous allons donc nous attacher à qualifier le litige en cause, à savoir notamment s'il relève du statut personnel au regard du droit québécois, du droit de l'Union européenne et plus particulièrement du droit français dans la mesure où le droit de l'Union européenne laisse aux États membres « le soin » de régir le droit des personnes, et du droit suisse (1.). Nous allons également s'interroger sur la nature contractuelle ou extracontractuelle/délictuelle d'un litige (2.), sur les lois de police appliquées aux données personnelles (3.), et enfin sur les sanctions applicables en cas d'atteintes aux données personnelles (4.).

1. Données personnelles et statut personnel

Le statut personnel « *regroupe l'ensemble des problèmes dans lesquels la personne se trouve non seulement impliquée (...), mais directement mise en cause. (...). Au statut personnel convient, (...), la loi personnelle, c'est-à-dire une loi qui présente un lien direct avec la personne ».*[80]

À cet égard, en droit québécois, l'article 3 du Code civil dispose que : « *Toute personne est titulaire de droits de la personnalité, tels le droit à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation et de sa vie privée.*

Ces droits sont incessibles ».[81]

Nous pouvons alors penser que le droit de la protection des données personnelles relève de la catégorie des droits extrapatrimoniaux en ce qu'ils sont notamment incessibles et donc de la responsabilité extracontractuelle, mais que le contenu du droit dépend du statut personnel. Monsieur le Professeur Gérald Goldstein a ainsi avancé l'idée que : « *(...) le rattachement de l'existence de ces droits fondamentaux pourrait s'effectuer par une qualification « statut*

[79] *Id.*
[80] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.367.
[81] *Code civil du Québec,* L.Q., 1991, c. 64., art.3.

personnel ». (…) Au contraire, la sanction et l'exercice de ces droits relèveraient de la loi applicable à la responsabilité civile (ou pénale) ».[82]

Ainsi, en droit québécois, la violation des données personnelles relève de la catégorie des droits extrapatrimoniaux, et est susceptible d'être sanctionnée sur le plan de la responsabilité civile extracontractuelle, mais le contenu du droit dépend du statut personnel.

En droit européen, la question de la qualification des données personnelles relève du droit interne de chaque État.

Par exemple, en droit français, « *(…) beaucoup d'auteurs voudraient faire entrer les droits de la personnalité. Mais la jurisprudence s'y montre, à juste titre réticente (…). Ne relèvent donc du statut personnel que le nom, la capacité, le mariage et la filiation ».*[83]

Le nom en droit français relève donc du statut personnel. À cet égard, l'article 3 alinéa 3 du Code civil dispose : « *Les lois concernant l'état et la capacité des personnes régissent les Français, même résidant en pays étranger ».*[84] Les sous-catégories de cet ensemble sont le nom, la capacité, le mariage et la filiation.[85]

Le statut personnel auquel convient la loi personnelle, la loi présentant un lien direct avec la personne concernée. En droit français la loi personnelle est donc la loi de la nationalité d'après l'alinéa 3 de l'article 3 du Code civil.[86]

Une partie de la doctrine française souhaite que les droits de la personnalité tel que le droit à l'image par exemple, entrent dans le domaine de la loi personnelle. Mais la jurisprudence « *centre son analyse, non sur le droit subjectif atteint, mais sur l'atteinte elle-même ».*[87]

Ainsi, concernant les autres atteintes aux données personnelles, autres que le nom, elles ne relèvent pas du statut personnel.

---

[82] GOLDSTEIN, G., GROFFIER, E., *Droit international privé: Tome II règles spécifiques,*Cowansville, Québec, éd. Yvon Blais,2003,1253p.
[83] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.367.
[84] *Code civil*, art. 3.
[85] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.367.
[86] *Id.*
[87] *Id.,* p.373.

La Cour de cassation française, en matière d'atteintes au droit à l'image, a dans un arrêt *Farah Diba*[88] affirmé la loi de l'État où la faute a été commise, c'est-à-dire la loi française, et non pris en compte la loi de nationalité de la victime, en l'espèce la loi iranienne.

En d'autres termes, la violation des données personnelles est considérée en droit français comme relevant de la catégorie des droits extrapatrimoniaux et donc susceptibles d'être sanctionnée sur le plan de la responsabilité civile. Seul le nom relève du statut personnel. Cependant, nous pouvons penser au regard de la doctrine et de la jurisprudence que le contenu du droit dépend du statut personnel.

En droit suisse, une préférence semble se dessiner autour de la responsabilité civile extracontractuelle/délictuelle.

À cet égard, Monsieur le Professeur Gérald Goldstein souligne le fait que « *la jurisprudence suisse avait dégagé une qualification délictuelle »*[89] des droits de la personnalité, et « *(…) cette jurisprudence a trouvé son chemin dans la loi de droit international privé ».*[90]

L'alinéa 2 de l'article 33 de la loi sur le droit international privé suisse dispose que : « *Toutefois, les atteintes aux intérêts personnels sont régies par les dispositions de la présente loi relatives aux actes illicites ».*[91]

Et l'article 139 de la même loi offre le choix à la victime entre plusieurs facteurs de rattachement, en cas d'atteintes aux droits de la personnalité par les médias et notamment par la voie de la presse.[92] Nous le verrons plus tard mais cette disposition « *illustre assez bien qu'il est possible, en formulant une règle de conflit de nature extracontractuelle adaptée, de répondre aux besoins actuels en ce domaine des droits de la personnalité ».* [93]

Autrement dit, en droit suisse, la violation du droit à la protection des données personnelles relève de la responsabilité extracontractuelle/délictuelle, et en même temps un choix entre différentes lois est laissé à la victime. Cela démontre une volonté de favoriser la

---

[88] Civ.1ère, 13 avril 1988, *Bull.civ*., n°98.
[89] GOLDSTEIN, G., GROFFIER, E., *Droit international privé: Tome II règles spécifiques,*Cowansville, Québec, éd. Yvon Blais,2003,1253p.
[90] *Id.*
[91] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art.33 al.2.
[92] *Id.*, art. 139.
[93] GOLDSTEIN, G., GROFFIER, E., *Droit international privé: Tome II règles spécifiques,*Cowansville, Québec, éd. Yvon Blais,2003,1253p.

victime et également de s'adapter, nous aborderons ce thème ultérieurement, à des situations prenant place sur internet.

Ainsi, en droit québécois, la violation des données personnelles relève de la responsabilité extracontractuelle/délictuelle, et selon la doctrine dont le Professeur Goldstein, le contenu du droit même relève du statut personnel.

En droit français, le régime du nom relève du statut personnel mais ce n'est pas le cas des autres atteintes aux données personnelles qui elles relèvent de la responsabilité extracontractuelle/délictuelle. Ce n'est toutefois pas le cas du nom qui relève du statut personnel : une atteinte au nom relèvera donc du statut personnel.

Quant au droit suisse, la violation des données personnelles relève de la responsabilité civile extracontractuelle/délictuelle et laisse à la victime d'une atteinte à ses données personnelles par la voie de presse, le choix entre plusieurs facteurs de rattachement.

Nous allons étudier les données personnelles au regard de la responsabilité civile contractuelle ou extracontractuelle/délictuelle. Dans le cas d'atteintes aux données personnelles, il semble bien évident que la responsabilité qui en relève soit de nature extracontractuelle/délictuelle mais dans certaines situations, que nous analyserons, cela est complexe et la question mérite d'être soulevée (2.).

2. Données personnelles et responsabilité civile contractuelle ou extracontractuelle

D'autre part, dans le cas où le litige en cause relève de la responsabilité civile, s'agit-il de la responsabilité civile extracontractuelle/délictuelle ou contractuelle ? La réponse à cette question semble pour le moins évidente, le litige relèvera de la matière extracontractuelle. Cependant, dans certaines situations la question peut se poser que ce soit en cas d'atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers (a.), des autres atteintes au droit de la protection des données personnelles (b.), ou concernant les atteintes prenant place uniquement sur internet (c.)

a. Atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers

Il parait possible de penser que deux entreprises qui échangent des informations relatives à des personnes passent un contrat ensemble et conviennent de la juridiction compétente et de la loi applicable en cas de violation de ces données personnelles.

Les données personnelles relèvent de la catégorie des droits extrapatrimoniaux et de ce fait ne peuvent faire l'objet d'un commerce, etc. L'échange de données à caractère personnel entre entreprises privées ne relèvera pas de la matière contractuelle, mais extracontractuelle.

b. Autres atteintes au droit de la protection des données personnelles

Concernant les autres violations aux données personnelles, nous pouvons nous sur la question du droit à l'image. À cet égard, le droit à l'image ou une photographie peut, selon les législations, faire l'objet d'un commerce, c'est-à-dire avoir un caractère patrimonial. Dès lors, en cas de litige, celui-ci peut être de nature contractuelle. Toutefois, nous pouvons alors penser que dans un cadre commercial, il ne s'agisse plus véritablement de données personnelles.

Ainsi, outre cette possibilité inhérente au droit à l'image, les données personnelles de manière générale ont un caractère extrapatrimonial, ce qui fait qu'elles ne peuvent faire l'objet de convention : la nature du litige en cause sera donc de nature extracontractuelle.

c. Atteintes au droit de la protection des données personnelles prenant place uniquement sur internet

En matière d'atteintes aux données personnelles prenant place uniquement sur internet, il est pertinent de s'interroger sur la nature de l'action, par exemple, en matière de contrats d'adhésion approuvés par les internautes lorsqu'ils s'inscrivent sur des réseaux sociaux. En cas de litige, l'utilisateur, en ayant souscrit au contrat d'adhésion, accepte et dès lors se soustrait aux conditions générales posées par les entreprises, à savoir le tribunal compétent et la loi applicable. Ce litige relève-t-il de la matière contractuelle ou délictuelle ?

Dans le cas d'autres atteintes inhérentes à internet, à savoir le « *spamming* », pourriel ou courriel indésirable, ou encore le « *spyware* », logiciel espion ou mouchard, le litige en cause relèvera de la matière délictuelle. En effet, aucun contrat n'est passé entre l'internaute et le tiers, auteur de la violation des données personnelles.

Toutefois, en matière de « *spamming* », le seul fait pour l'utilisateur d'avoir consenti à l'envoi de courriel commercial, suffit-il à qualifier un litige, s'il a lieu, de contractuel ? De la même façon en ce qui concerne les « *cookies* » ou témoins de connexion ? Le consentement de l'internaute à poursuivre la navigation sur un site internet utilisant des « *cookies* » permet-il de qualifier l'action en cause de contractuelle ?

Il est fort à penser que dans la mesure où les données personnelles relèvent des droits extrapatrimoniaux, la nature du litige sera de nature extracontractuelle.

Nous pouvons donc penser que l'utilisation non permise d'une donnée personnelle dans le cadre d'un contrat sur internet sera « hors » contrat et relèvera donc de la responsabilité extracontractuelle/délictuelle.

L'utilisation des données personnelles faite par une des parties au contrat sans le consentement de l'intéressé, que ce soit par le biais des flux transfrontaliers ou par le biais de contrats sur internet, engage de la responsabilité extracontractuelle/délictuelle et non plus contractuelle de l'auteur du dommage. D'autre part, dans le cas de la marchandisation d'une photographie, nous pouvons légitimement penser que le caractère commercial ne donne plus lieu à la notion de donnée personnelle : ce n'est que si l'image est utilisée sans le consentement de l'intéressé que le litige relèvera alors de la responsabilité extracontractuelle/délictuelle.

Nous allons étudier les lois de police qui pourraient s'appliquer en cas d'atteintes aux données personnelles (3.).

3. Données personnelles et lois de police

L'auteur Francescakis définissait les lois de police comme étant des lois dont « *l'observation est nécessaire pour la sauvegarde de l'organisation politique, sociale et économique du pays* ».[94]

Il convient de préciser que « *la loi de police doit donc être appliquée sans avoir égard à la règle de conflit de lois* ».[95] Il s'agit de règles protectrices susceptibles de s'appliquer :

[94] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.99.

lorsqu'une règle du for « *(...) indique qu'elle doit être appliquée aux questions de droit présentant un certain rattachement, qu'elle précise avec l'État du for. (...) Sinon, il faut déterminer les cas dans lesquels son application est nécessaire pour que le but cherché soit atteint ».*[96] De ce fait, « *toute loi de police possède ainsi un domaine d'application nécessaire déduit de l'objectif qu'elle poursuit ».*[97]

Le juge saisi du litige pourrait mettre en avant la nécessité de protéger les données personnelles, et ainsi l'ériger en loi de police. La protection des données personnelles, en ce qu'il est question d'un sujet particulièrement sensible et touchant chaque individu, pourrait être érigé en lois de police.

Il est donc tout à fait possible d'envisager les lois de police dans le cas où la protection des données personnelles est considérée comme impérative.

Nous allons nous intéresser aux différentes sanctions envisageables en cas d'atteintes aux données personnelles (4.).

4. Sanctions

En matière de responsabilité civile extracontractuelle/délictuelle, les sanctions peuvent consister en une obligation de réparer en nature (ce qui peut s'avérer difficile lorsque cela concerne des cas de violations des données personnelles), ou une réparation par équivalent qui correspond de manière générale à l'allocation de dommages et intérêts eu égard au préjudice subi.

En d'autres termes, les sanctions seront soit la réparation en nature, soit l'allocation de dommages et intérêts.

Nous allons étudier les objectifs des règles de droit international privé au regard des données personnelles (B.). Cette partie est importante dans la mesure où elle permet de comprendre quels sont les principaux objectifs auxquels les juges en charge du litige doivent

---

[95] *Id,* p.101.
[96] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.101.
[97] *Id.*

répondre afin de se déclarer compétent pour trancher un litige et ensuite déterminer la loi applicable.

B. Données personnelles et objectifs des règles de droit international privé

Nous allons nous intéresser aux objectifs poursuivis en matière de compétence juridictionnelle (1.) puis en matière de conflits de lois (2.).

1. Données personnelles et compétence juridictionnelle

La détermination de la situation litigieuse dans le cadre de la compétence juridictionnelle, c'est-à-dire l'opération de qualification et les critères de rattachement qui en découlent, doit avoir pour objectifs principaux la bonne administration de la justice, la prévisibilité des règles de compétence vis-à-vis du défendeur et l'équité procédurale. D'autre part, il doit exister des liens suffisants, significatifs entre le litige et les juridictions saisies.

Le respect du principe de bonne administration de la justice a pour objectif d'éviter la multiplication des juridictions compétentes. Seul un tribunal doit être compétent pour connaitre du litige et cela notamment afin d'éviter une multiplicité des décisions rendues et les risques d'incompatibilité des décisions. Nous pouvons imaginer en matière de protection des données personnelles, et notamment en cas d'atteintes sur internet, qu'une multitude de tribunaux se déclarent compétents dans le cas où le préjudice par exemple, est subi par la victime dans un grand nombre d'États. Or, le respect du principe de bonne administration de la justice voudra qu'un seul tribunal se déclare compétent.[98]

Le principe de prévisibilité des règles de compétence vis-à-vis du défendeur est assez logique : le défendeur doit pouvoir s'attendre à être attrait devant telle ou telle juridiction.

L'équité procédurale : aucune des parties au litige ne doit être favorisée au détriment d'une autre. Le for saisi ne doit pas privilégier une partie au détriment d'une autre.

---

[98] SINOPOLI, L., *Le procès équitable dans les rapports privés internationaux – Recherche sur le champ d'application de l'article 6 paragraphe 1re de la Convention européenne des droits de l'homme en droit international privé*, Thèse, Paris, Université Paris 1 Panthéon-Sorbonne, 2000.

Et enfin l'existence de liens suffisants entre le litige et les juridictions saisies est assez logique : un tribunal ne pourra pas se déclarer compétent si le litige en cause ne présente aucun lien significatif avec les juridictions de l'État.

Nous allons à présent nous intéresser aux objectifs principaux inhérents aux règles de conflits de lois (2.).

2. Données personnelles et règles de conflits de lois

En ce qui concerne les règles de conflits de lois, les objectifs principaux sont la prévisibilité et le principe de proximité.

S'agissant de la prévisibilité, l'objectif principal recherché par la règle de conflit de lois est « *(...) le respect des légitimes prévisions des parties* ».[99] C'est-à-dire que telle ou telle loi sera applicable dès lors que les parties au litige pouvaient légitimement s'attendre à ce que ce soit cette loi et non une autre qui soit applicable. Autrement dit, si la situation n'a aucun rapport avec le for saisi, sa règle de conflit n'aura pas vocation à s'appliquer eu égard à l'éloignement du for avec la situation.[100]

Quant au principe de proximité, le tribunal initialement saisi appliquera, non pas sa propre règle de conflit de lois, mais la règle de conflit d'un autre tribunal plus compétent pour juger du litige car il présente des liens plus étroits avec le litige.[101] Cela peut être la prise en compte de l'État de la nationalité du demandeur et/ou du défendeur à l'Instance, du l'État de commission de la faute, de l'État où le préjudice a été subi, de l'État du domicile de la victime et/ou de l'auteur du dommage etc.

Chaque critère de rattachement étudié dans les deux chapitres suivants sera étudié en fonction de ces principes. La ou les meilleure(s) solution(s) en matière de compétence juridictionnelle ou de conflits de lois dépendra donc du respect de l'ensemble de ces principes.

De manière générale, nous pouvons penser que les données personnelles relèvent du statut personnel lorsqu'il est question du contenu du droit puisque cela touche la personne, et de la

---

[99] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, p.173.
[100] *Id.*
[101] *Id.*

responsabilité extracontractuelle, lorsqu'il est question de la violation de l'obligation légale de ne pas nuire à autrui ou encore des lois de police si la protection des données personnelles est considérée comme impérative.

La nature contractuelle du litige en cas d'atteintes aux données personnelles ne vient finalement pas à se poser dans la mesure où si l'utilisation d'une donnée personnelle est faite sans le consentement de l'intéressé cela ne relèvera plus du contrat mais de l'extracontractuel/délictuel. Et concernant la monétisation de son image, le simple fait de commercialiser sa photographie fait qu'il ne s'agit plus véritablement d'une donnée personnelle.

Enfin, la sanction sera souvent la réparation en nature ou l'allocation de dommages et intérêts.

Synthèse

Il convient de revenir sur les différents points abordés dans le cadre de ce chapitre préliminaire.

Tout d'abord, en ce qui concerne le débat « vie privée et données personnelles », on se rend compte à travers cette analyse que ce qui est large ou étroit selon les systèmes juridiques, ce n'est pas tant la notion de données personnelles mais plutôt celle de vie privée. Cette différence d'approche peut certainement s'expliquer par l'approche plus intrusive du droit de l'Union européenne dans la vie privée des personnes, contrairement en Amérique du Nord où la notion de vie privée est perçue de manière beaucoup plus libérale. Toutefois, la vie privée ne relève pas ici de l'étude du sujet.

La définition générale que nous pouvons donner à la notion de « données » est la suivante : les « données personnelles » comprennent un nombre important d'informations qui peuvent être par exemple le nom, le prénom, une photographie, un numéro de téléphone, une date de naissance, une adresse postale mais également une adresse courriel ou encore le numéro d'assurance sociale. Il s'agit de « données » susceptibles d'identifier directement ou indirectement une personne.

Afin que la délimitation du sujet soit claire et précise, les données personnelles ne doivent pas être associées aux cas de diffamation dans la mesure où les atteintes au droit de la protection des données personnelles consistent en la divulgation d'élément permettant l'identification d'une personne, alors que la diffamation correspond au fait de tenir des propos, d'alléguer des faits précis pouvant porter atteinte à la réputation et à l'honneur d'un individu, ce qui est différent.

Concernant l'encadrement législatif des données personnelles : nous remarquons qu'en droit québécois et en droit suisse, la protection des données personnelles est sous la régie du droit au respect de la vie privée. En droit européen, la définition de la notion est donnée par les textes européens mais la protection est régie par le droit interne des États membres.

S’agissant de la matérialisation des données personnelles prenant place hors et sur internet, elle est relativement variée dans la mesure où l’atteinte peut arborer un caractère commercial en revendant des fichiers entre entreprises contenant des données personnelles par le biais des flux transfrontaliers, une intention de nuire à autrui par la diffusion d’une photographie ou de tout élément permettant l’identification d’un individu ou encore avoir un caractère frauduleux avec l’usurpation d’identité ou la fraude à la carte bancaire notamment.

Concernant les méthodes générales en droit international privé, et notamment la qualification à attribuer aux données personnelles, nous pouvons penser que les données personnelles relèvent du statut personnel lorsqu’il est question du contenu du droit puisque cela touche la personne, et de la responsabilité extracontractuelle, lorsqu’il est question de la violation de l’obligation légale de ne pas nuire à autrui ou encore des lois de police si la protection des données personnelles est considérée comme impérative.

Enfin, chaque critère de rattachement qui sera étudié dans les deux chapitres suivants sera étudié en fonction de ces principes : la ou les meilleure(s) solution(s) en matière de compétence juridictionnelle ou de conflits de lois dépendra donc du respect de l’ensemble de ces principes.

Le Chapitre 1 sera consacré à la compétence internationale des tribunaux en droit québécois, européen et suisse, puis le Chapitre 2 aux conflits de lois au regard des données personnelles.

Chapitre 1 : Données personnelles et compétence internationale des tribunaux en droit québécois, européen et suisse

Un litige impliquant la violation du droit à la protection des données personnelles relèvera de la responsabilité civile extracontractuelle/délictuelle.

Nous allons mettre en avant les facteurs de rattachement relatifs aux données personnelles en matière de compétence juridictionnelle. À cet égard, les flux transfrontaliers seront traités en même temps que les autres cas d'atteintes aux données personnelles, et le cas échéant, particularisés.

Les objectifs poursuivis étant encore une fois la bonne administration de la justice, la prévisibilité des règles de compétence vis-à-vis du défendeur, l'équité procédurale et l'existence de liens suffisants, significatifs entre le litige et les juridictions saisies.[102]

Plusieurs critères de rattachement peuvent être mis en avant, à savoir : le tribunal du lieu du préjudice (section 1), le tribunal du lieu de la faute (section 2), le tribunal du lieu du domicile du défendeur (section 3), le tribunal de l'État du domicile de la victime (section 4).

Pour chacun de ces facteurs, le droit commun (A), l'application aux données personnelles (B), puis la situation sur internet (C) seront étudiés. Les avantages et inconvénients de ces critères seront envisagés d'une part, dans le cadre de l'application aux données personnelles, puis d'autre part lors de l'application aux données personnelles sur internet. Toutefois, lorsque la situation sur internet ne change pas, les avantages et inconvénients ne seront pas présentés.

À cet égard, sur internet, la plupart des systèmes juridiques n'envisagent pas de règles de compétence juridictionnelle particulières sur internet.

En droit québécois par exemple, même si cet exemple ne concerne pas les données personnelles en tant que telles, « *(…) Tous les délits (diffamation, etc.) sont régis par les*

---

[102] MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007.

mêmes règles (...). Il n'existe pas de règle spéciale pour les « cyber-délits ». Le tribunal québécois du lieu de survenance du fait dommageable ou de commission de la faute est compétent de ce chef, tout comme celui où le préjudice a été subi ».[103]

Il existe cependant des critères de rattachement prenant place uniquement sur internet, qui ne relèvent pas du droit commun mais ont été envisagés ou non, par la doctrine. C'est notamment le cas du tribunal du centre des intérêts du demandeur qui a été mis en avant par la Cour de Justice de l'Union européenne en matière de diffamation (section 5). Même si ce cas d'espèce ne relève pas de la notion de données personnelles, il parait néanmoins intéressant de l'étudier.

D'autres critères ont été soulevés ou non par la doctrine : l'accessibilité (section 6), le ciblage (section 7), le lieu de localisation du serveur informatique (section 8), ou le lieu de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires (section 9).

Pour chacun de ces facteurs de rattachement, une présentation générale du critère (A), l'application aux données personnelles avec les avantages et inconvénients (B) seront analysés. La situation sur internet n'est ici pas nécessaire dans la mesure où il s'agit de critères envisageables uniquement sur internet.

Enfin nous allons étudier le forum « *non conveniens* », c'est-à-dire le déclinement de compétence d'une juridiction au profit d'un autre tribunal mieux à même de trancher le litige, même s'il ne s'agit pas d'un facteur de rattachement dans la mesure où cela relève de l'exercice même de la compétence et non pas de son existence (section 10). Pour cette section un peu particulière, nous allons nous intéresser au droit commun (A.), l'appliquer aux données personnelles (B.), puis envisager la situation sur internet (C.).

[103] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*

Section 1. Le tribunal du lieu du préjudice

A. Droit commun

En droit québécois, l'alinéa 3 de l'article 3148 du Code civil[104] dispose que : « *Dans les actions personnelles à caractère patrimonial, les autorités québécoises sont compétentes dans les cas suivants : 3. Une faute a été commise au Québec, un préjudice y a été subi, un fait dommageable s'y est produit ou l'une des obligations découlant d'un contrat devait y être exécutée* ».

En droit européen, l'article 7.2) du Règlement Bruxelles 1 Bis stipule que : « *Une personne domiciliée sur le territoire d'un État membre peut être attraite, dans un autre État membre : 3. En matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire* ».[105]

Dans un arrêt Mines de Potasse d'Alsace, la Cour a précisé que : « *Dans le cas où se situe le fait susceptible d'entrainer une responsabilité délictuelle ou quasi délictuelle et le lieu où ce fait a entrainé un dommage ne sont pas identiques, l'expression « lieu où le fait dommageable s'est produit ». L'article 5.3°, de la convention du 27 septembre 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, doit être entendu en ce sens qu'elle vise à la fois le lieu où le dommage est survenu et le lieu de l'évènement causal. Il en résulte que le défendeur peut être attrait, au choix du demandeur, devant le tribunal soit du lieu où le dommage est survenu, soit du lieu de l'évènement causal qui est à l'origine de ce dommage* ».[106]

Autrement dit dans cet arrêt, la Cour de Justice considère qu'en matière extracontractuelle/délictuelle, le demandeur peut également être attrait devant le tribunal du lieu où le préjudice est survenu, et non pas uniquement devant le tribunal du lieu où la faute a été commise.

---

[104] *Code civil du Québec,* L.Q., 1991, c. 64, art.3148.
[105] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).
[106] *Handelskwekerig G.J. Bier BV c. Mines de Potasse d'Alsace SA.,* Affaire C-21/76, CJCE, 30 novembre 1976, en ligne :
<http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:61976CJ0021&from=FR> (consulté le 20 septembre 2015).

En droit suisse, l'article 129 alinéa 1 de la loi fédérale sur le droit international privé dispose que : « *(…). Sont en outre compétents les tribunaux suisses du lieu (…) du résultat ».*[107]

Les tribunaux suisses seront donc compétents dès lors que le « résultat » de l'acte illicite a été subi en Suisse.

D'autre part, en droit suisse un autre texte peut être cité. En effet, la Convention de Lugano[108] est une convention internationale signée entre l'Union européenne et certains pays (Suisse, Norvège, Islande et Danemark) en matière de compétence internationale des tribunaux. Cette Convention reprend pour la plupart les règles déjà applicables en matière de compétence juridictionnelle prévues par le Règlement Bruxelles 1 Bis.[109] Elle a vocation à remplacer la loi sur le droit international privé en ce qui concerne la compétence juridictionnelle dans la mesure où les conventions internationales priment sur le droit international privé suisse.

L'article 5.3 de la Convention de Lugano stipule donc: « *Une personne domiciliée sur le territoire d'un État lié par la présente Convention peut être attraite, dans un autre État lié par la présente convention : 3. En matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ».*[110] Nous pouvons alors penser que la jurisprudence Mines de Potasse d'Alsace[111] dans laquelle la Cour de Justice considère que « *le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire* » s'entend aussi bien comme le tribunal de l'État de la faute mais également le tribunal de l'État du préjudice, s'applique également à cette disposition.

Cette disposition reprend les mêmes termes que l'article 7.2) du Règlement Bruxelles 1 Bis.[112]

---

[107] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 129 al.1.

[108] Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne : < https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html > (consulté le 29 octobre 2015).

[109] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).

[110] Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne : < https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html > (consulté le 29 octobre 2015).

[111] *Handelskwekerig G.J. Bier BV c. Mines de Potasse d'Alsace SA.,* Affaire C-21/76, CJCE, 30 novembre 1976, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:61976CJ0021&from=FR> (consulté le 20 septembre 2015).

[112] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).

B. Application aux données personnelles

En droit québécois, l'article 3148 alinéa 3 du Code civil pourrait donc être applicable en cas d'atteinte au droit à l'image d'une personne. En effet, le droit à l'image peut revêtir un double aspect puisqu'il peut être patrimonial ou extrapatrimonial : « *dans la plupart des pays, le droit des personnes à exercer un contrôle sur la diffusion de leur image comporte une double facette selon que l'image est utilisée à des fins mercantiles ou à des fins d'information légitime du public. C'est pourquoi le droit à l'image a un double aspect. Un aspect patrimonial, c'est-à-dire appréciable en argent et un aspect extrapatrimonial, c'est-à-dire qui ne s'évalue pas en terme de valeur pécuniaire* ».[113] Ainsi, une personne peut choisir de « monnayer » son image, c'est-à-dire utiliser son image afin de percevoir de l'argent. L'exemple le plus évocateur est celui de la « personnalité publique » : elle peut signer un contrat afin d'être photographiée par un magazine et percevoir en échange une contrepartie financière ; néanmoins lorsque ce n'est pas le cas, c'est-à-dire lorsqu'il s'agit de photographies prises à l'insu de la personne, c'est-à-dire sans son consentement, l'article 3148 du C.c.Q. ne sera ici pas applicable puisque le droit à l'image n'aura plus un aspect patrimonial mais extrapatrimonial.

Cependant, nous pouvons alors penser que dans un « cadre commercial », il n'est plus question de « données personnelles » mais de « monétisation » de l'image.

Concernant les autres types d'atteintes aux données personnelles, celles-ci n'ayant pas un caractère patrimonial, elles ne sont dès lors pas concernées par cette disposition.

---

[113] TRUDEL, P., *Notes du cours* DRT 3805G (*Droit des technologies de l'information*), Montréal, en ligne : < http://www.chairelrwilson.ca/cours/drt3805g/image.html > (consulté le 6 mars 2015).

En droit européen, l'article 7.2 bis du Règlement Bruxelles 1 Bis[114] est applicable à la matière extracontractuelle/délictuelle. Dès lors, la victime d'une atteinte au droit à l'image, à ses nom, prénom ou toutes informations personnelles permettant d'identifier un individu peut saisir les juridictions de l'État où le préjudice est survenu.

En droit suisse, l'article 129 al.1 de la loi fédérale[115] est applicable aux « actes illicites », dès lors de la même façon qu'en droit de l'Union européenne, la victime d'une violation au droit à la protection de ses données personnelles pourra saisir le tribunal de l'État où le préjudice est survenu.

Quant à la disposition de la Convention de Lugano,[116] celle-ci reprend l'article 7.2. bis du Règlement Bruxelles 1 Bis [117] applicable à la matière extracontractuelle.

Dans le cas de la diffusion d'une image sans l'autorisation préalable de la personne intéressée par une tierce personne, la victime peut saisir le tribunal de l'État où le préjudice est survenu. Dès lors, de quelle façon se concrétise « la survenance » du préjudice ? Cela pourrait s'apparenter au(x) lieu(x) où l'image a été diffusée ou au lieu où l'atteinte au droit à l'image a été commise.

Avantages et inconvénients

La possibilité pour la victime de saisir le tribunal du lieu du préjudice est survenue lui permet d'éviter un déplacement impliquant un coût financier ainsi qu'une perte de temps.

Il peut paraitre logique que la victime d'une atteinte n'ait pas à subir un coût et une perte de temps inhérent à un déplacement afin de saisir les tribunaux d'un autre État. À cet égard, le demandeur subi déjà un préjudice et doit tout de même se rendre dans un autre État pour pouvoir obtenir, le cas échéant, réparation.

---

[114] *CE*, *Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).
[115] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 129 al.1.
[116] Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne :
< https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html > (consulté le 29 octobre 2015).
[117] *CE*, *Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).

Les inconvénients liés au choix du tribunal du lieu où le préjudice a été subi semblent davantage être préjudiciable au défendeur.

À cet égard, plusieurs éléments peuvent être mis en avant concernant les atteintes susceptibles d'être portées aux droits de la partie défenderesse.

Tout d'abord, ce choix de compétence du tribunal est imprévisible pour le défendeur à l'instance. En effet, il n'est pas forcément facile d'établir une prévisibilité du lieu où le préjudice va être subi par la victime.

D'autre part, le tribunal du lieu où le préjudice a été subi peut être différent du lieu où l'auteur de l'acte dommageable a sa résidence principale : ce qui peut obliger le défendeur à se déplacer devant les tribunaux d'un autre état, et ainsi lui entrainer des coûts supplémentaires, ainsi qu'une perte de temps. Or ces deux inconvénients sont d'autant plus préjudiciables à l'égard de l'auteur de l'acte lorsque la faute ne lui est pas imputable.

Enfin, ce critère de rattachement peut avoir pour conséquence un risque de « *forum shopping* » dans la mesure où le préjudice peut être subi dans différents États. Or s'il y a plusieurs lieux, le demandeur à l'espèce peut alors choisir de saisir le tribunal de l'État en fonction de la loi que celui-ci est susceptible d'appliquer.

Dans le cas d'une atteinte au droit de la protection des données personnelles par le biais des flux transfrontaliers, contrairement à la diffamation par exemple, il semble que le préjudice ne soit localisable qu'au sein du même État, mais cela dépend bien évidemment de la manière dont l'information a été transmise. Il peut donc y avoir un responsable de l'information et également un sous-traitant en charge de sa gestion localisé dans des États différents et donc le préjudice peut être subi dans différents États.

C. Situation sur internet

D'après la doctrine québécoise, le seul fait que : « *(...) le dommage a été subi au Québec suffit pour déclencher la compétence du tribunal, en cas de diffamation, par internet*

ou non, comme dans les autres hypothèses de responsabilité civile, même si cette atteinte ne fut pas intentionnelle ou si l'auteur ne visait pas spécifiquement le Québec ».[118]

Sur internet, le tribunal de l'État du lieu de survenance du préjudice revient à prendre en considération la loi de l'État de réception de l'information ou « *downloading* ».

Il s'agit donc d'étudier les éventuelles spécificités concernant la réception de l'information au regard des données personnelles sur internet.

Avantages et inconvénients sur internet

Cette solution présente un aspect équitable à l'égard de la victime puisque cette dernière ne se verra pas dans l'obligation d'attraire l'auteur du dommage devant le tribunal du lieu de sa résidence principale ou celui du lieu de la faute : seul sera compétent le tribunal du lieu où le préjudice a été subi par le demandeur à l'instance. Cela permet donc d'éviter des coûts relatif au déplacement et une perte de temps.

Il semble donc que cette solution, à savoir le tribunal du lieu du préjudice, présente les mêmes avantages dans le cadre d'une situation normale et sur internet.

À contrario, les inconvénients semblent être ici accentués avec l'apparition de l'Internet.

À cet égard, la localisation d'une atteinte aux données personnelles sur internet parait difficile dans la mesure où une violation des données personnelles sur la toile peut être localisée dans un nombre d'États importants.

L'auteur du dommage peut donc être attrait par le demandeur à l'instance devant l'ensemble des tribunaux des pays où l'information est accessible sur internet, et cela peut donc laisser une place au « *forum shopping* » : la victime choisit de saisir le tribunal de l'État susceptible de rendre une décision qui lui sera favorable.

---

[118] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*

De plus, le tribunal du lieu où le préjudice est subi présente un aspect imprévisible à l'égard de l'auteur du dommage qui s'intensifie avec internet puisque le défendeur est susceptible d'être attrait devant plusieurs juridictions.

D'autre part, quand la victime est censée avoir reçu l'information sur internet ? Que signifie la notion de « réception » ? Il convient de préciser que le lieu de l'État de réception peut être assimilé au lieu où la victime reçoit le message, c'est-à-dire l'État où elle prend connaissance de l'information. Il ne s'agit pas de prendre en compte les différents lieux dans lesquels la victime est susceptible de subir un dommage mais seulement du lieu où la victime prend connaissance de ce message. Or ce lieu peut être différent du lieu où la victime subit réellement l'atteinte aux données personnelles. Dès lors, dans le cas où la victime se trouve dans un État X (voyage d'affaires ou autres), cela signifie-t-il que ce sera les juridictions de l'État X qui seront compétentes ? Cela impliquerait une forte imprévisibilité à l'égard du défendeur à l'instance.

Les mêmes avantages et inconvénients en ce qui concerne le non-respect du droit à la protection des données personnelles et les cas d'atteintes aux données personnelles par le biais des flux transfrontaliers peuvent être mis en avant sur internet.

Cette solution est juste et équitable à l'égard de la victime mais imprévisible à l'encontre de l'auteur du dommage puisque le préjudice peut être subi dans plusieurs États.

Sur internet, les inconvénients peuvent être accentués : une atteinte au droit de la protection des données personnelles peut être localisée dans de nombreux États.

Section 2. Le tribunal du lieu de la faute

A. Droit commun

En droit québécois, l'alinéa 3 de l'article 3148 du C.c.Q. dispose que : « *Dans les actions personnelles à caractère patrimonial, les autorités québécoises sont compétentes dans les cas suivants : 3. Une faute a été commise au Québec, un préjudice y a été subi, un fait*

dommageable s'y est produit ou l'une des obligations découlant d'un contrat devait y être exécutée ».[119]

En droit de l'Union européenne, l'article 7.2) du Règlement Bruxelles 1 Bis stipule que : « *Une personne domiciliée sur le territoire d'un État membre peut être attraite, dans un autre État membre : 3. En matière délictuelle ou quasi-délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ».*[120]

En droit suisse, l'article 129 alinéa 1 de la loi fédérale sur le droit international privé dispose que : « *(…) Sont en outre compétents les tribunaux suisse du lieu de l'acte (…) ».*[121]

Et l'article 5.3 de la Convention de Lugano : « *Une personne domiciliée sur le territoire d'un État lié par la présente Convention peut être attraite, dans un autre État lié par la présente convention : 3. En matière délictuelle ou quasi délictuelle, devant le tribunal du lieu où le fait dommageable s'est produit ou risque de se produire ».*[122]

B. Application aux données personnelles

En matière de données personnelles, le tribunal compétent sera le tribunal où l'atteinte au droit de la protection des données personnelles a été commise. En d'autres termes, si le défendeur à l'instance viole le droit à l'image d'une personne ou publie les informations personnelles d'un individu, ce sera le lieu où la faute c'est-à-dire la diffusion ou/et la publication des informations a été commise.

Cependant, en droit québécois encore une fois, l'application aux données personnelles semble difficile. En effet, dans la mesure où il s'agit d'« *actions personnelles à caractère patrimonial* »,[123] l'application aux données personnelles n'est pas envisageable. Le droit à

---

[119] *Code civil du Québec*, L.Q. 1991, c.64, art.3148.
[120] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).
[121] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 129 al.1.
[122] Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne :
< https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html > (consulté le 29 octobre 2015).
[123] *Code civil du Québec*, L.Q. 1991, c.64, art.3148.

l'image pouvant certes être « monétisé », mais une fois monétiser il paraît difficile de parler de données personnelles.

Avantages et inconvénients

Le principal avantage est l'aspect prévisible de ce critère à l'égard du défendeur à l'instance.

De plus, le tribunal de l'État de survenance de la faute permet d'éviter la possibilité d'une multiplicité des recours de la part de la victime.

Plusieurs inconvénients peuvent ici être mis en avant concernant le choix du tribunal du lieu de la faute.

Tout d'abord, ce critère peut paraitre injuste à l'égard de la victime. À cet égard, il est possible de noter que le lieu de la faute soit différent du lieu où la victime a son domicile principal ou tout du moins du lieu où cette dernière a subi un préjudice portant atteinte au droit à la protection de ses données personnelles. Dès lors, le demandeur à l'instance est, d'une part victime d'une atteinte à ses droits, et d'autre part, va être contraint de se déplacer et ainsi saisir le tribunal de l'État où la faute a été commise : cela peut engendrer un coût supplémentaire mais également une perte de temps à ne pas négliger. Or eu égard à ces différentes barrières érigées à l'encontre du demandeur, ce dernier peut choisir de ne pas saisir les juridictions, c'est-à-dire de ne pas engager une action civile malgré le préjudice subi.

D'autre part, il est possible d'imaginer que le défendeur en l'espèce peut être tenté de choisir le tribunal de l'État où il commettra une violation des données personnelles, en fonction de la loi que ce tribunal sera susceptible d'appliquer.

Les mêmes avantages et inconvénients peuvent être identifiés en cas de non-respect au droit de la protection des données personnelles et d'atteintes aux données personnelles par le biais des flux transfrontaliers.

C. Situation sur internet

Sur internet, le tribunal de l'État de survenance de la faute revient à prendre en considération le tribunal de l'État de l'émission ou de transmission de l'information, « *uploading* ».

Il s'agit de s'intéresser ici aux éventuelles spécificités pouvant prendre place sur internet.

Avantages et inconvénients sur internet

En ce qui concerne les avantages, aucune spécificité sur internet n'est à relever.

Le principal désavantage concerne la matérialisation de la faute lorsqu'il s'agit d'une violation du droit à la protection des données personnelles commise sur internet. En effet, de quelle manière est-il possible de localiser une faute prenant place sur internet ? Convient-il de prendre en compte la localisation du serveur ? Le lieu de connexion, c'est-à-dire l'État où la connexion à internet a été établie suite à la survenance de la faute ? Ou au contraire, s'agit-il de prendre en compte des critères physiques, à savoir par exemple, le lieu de la résidence principale du défendeur, tel que précédemment étudié ?

À cet égard, et notamment pour éviter que l'auteur du dommage choisisse volontairement de commettre un dommage dans un autre État (notamment par le biais d'un serveur localisé dans un État autre que celui de sa résidence principale) aux fins d'éviter l'application de certaines législations considérées comme contraignantes en matière de violation du droit à la protection des données personnelles, il conviendrait de prendre en compte des critères hors internet.

La solution la plus appropriée et plus juste serait donc la prise en compte du tribunal de l'État où l'auteur du dommage se trouve « physiquement » au moment de la violation des données personnelles.

Toutefois, un point important doit ici être soulevé : le fait de prendre en compte le lieu où l'auteur du dommage a commis « physiquement » son atteinte ne permet pas d'éviter des abus de la part de ce dernier. En effet, il parait légitime de penser que le défendeur à l'instance pourrait s'établir « physiquement » dans un autre État, et cela de manière temporaire, aux fins d'éviter les législations de son État de résidence principale. Or, cette possibilité offerte à l'égard du défendeur peut paraitre profondément injuste à l'égard de la victime.

De la même façon les mêmes avantages et inconvénients peuvent être mis en avant en cas de non-respect au droit de la protection des données personnelles et des flux transfrontaliers sur internet.

Ce critère de rattachement est envisageable dans la mesure où il respecte le principe de prévisibilité à l'égard de l'auteur du dommage. Cependant, cette solution est injuste et inéquitable envers la victime : l'auteur pouvant choisir de commettre une faute dans un État en fonction de la loi que le tribunal de cet État saisi appliquera.

Sur internet, la situation est identique à celle hors internet.

Section 3. Le tribunal de l'État du domicile du défendeur

A. Droit commun

En droit québécois, l'alinéa 1 de l'article 3148 du Code civil dispose que : « *Dans les actions personnelles à caractère patrimonial, les autorités québécoises sont compétentes dans les cas suivants : 1. Le défendeur a son domicile ou sa résidence au Québec ».*[124]

D'autre part, l'article 3141 du C.c.Q. stipule que : « *Les autorités du Québec sont compétentes pour connaitre des actions personnelles à caractère extrapatrimonial et familial, lorsque l'une des personnes concernées est domiciliée au Québec ».*[125]

En d'autres termes, qu'il s'agisse d'une action à caractère patrimonial ou extrapatrimonial, le tribunal du lieu du domicile du défendeur peut être compétent.

En droit européen, l'article 4 du Règlement Bruxelles 1 Bis prévoit que : « *1. Sous réserve des dispositions du présent règlement, les personnes domiciliées sur le territoire d'un État membre sont attraites, quelle que soit leur nationalité, devant les juridictions de cet État membre ».*[126]

---

[124] *Code civil du Québec*, L.Q. 1991, c.64, art. 3148.
[125] *Id.,* art. 3141.
[126] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).

En d'autres termes, le demandeur à l'instance a le choix d'attraire le défendeur à l'instance devant le tribunal du lieu de son domicile.

En droit suisse, l'article 129 alinéa 1 de la loi fédérale sur le droit international privé dispose que : *«Les tribunaux suisses du domicile ou, à défaut de domicile, ceux de la résidence habituelle du défendeur sont compétents pour connaitre des actions fondées sur un acte illicite».*[127]

Autrement dit, lorsqu'aucune disposition spécifique ne vient à s'appliquer, ce sera le tribunal de l'État du domicile du défendeur à l'instance qui sera compétent.

D'autre part, l'article 2 alinéa 1 de la Convention de Lugano prévoit que : « *Sous réserve des dispositions de la présente Convention, les personnes domiciliées sur le territoire d'un État lié par la présente Convention sont attraites, quelle que soit leur nationalité, devant les juridictions de cet État ».*[128]

Cette disposition reprend donc l'article 4 du Règlement Bruxelles 1 Bis.[129]

B. Application aux données personnelles

Appliqué aux données personnelles, ce critère de rattachement ne présente pas de réelles spécificités : le tribunal compétent sera le tribunal de l'État où l'auteur de l'atteinte a son domicile.

Avantages et inconvénients

Le principal avantage semble être le caractère prévisible à l'égard de l'auteur d'une atteinte au droit à la protection des données personnelles. En effet, le demandeur à l'espèce peut légitimement s'attendre à être attrait devant les tribunaux où ce dernier est domicilié.

---

[127] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 129 al.1.
[128] Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne :
< https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html > (consulté le 29 octobre 2015).
[129] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).

D'autre part, cela permet d'éviter les cas de multiplicité des recours puisque le seul tribunal compétent aux fins de trancher le litige sera le tribunal du lieu où le défendeur a son domicile.

Toutefois, ce facteur de rattachement peut paraitre particulièrement injuste à l'égard de la victime.

Tout d'abord, si le demandeur en l'espèce réside dans un État différent que le défendeur, ce dernier aura alors à se déplacer dans cet autre État. Or ce déplacement est susceptible d'impliquer des coûts supplémentaires non négligeables, eu égard notamment à la distance géographique entre les États. Cela peut avoir un effet dissuasif à l'égard du demandeur qui choisira de ne pas porter le litige devant le tribunal d'un autre État en raison de la distance mais aussi du temps que cela peut engendrer.

D'autre part, il est possible de supposer que le défendeur choisisse délibérément de commettre un acte portant atteinte au droit de la protection des données personnelles d'un individu dans son État de résidence dans la mesure où le tribunal sera susceptible de rendre une décision favorable à son égard.

Il est évident que la désignation du tribunal de l'État où le défendeur a sa résidence principale est moins flexible que celle du tribunal de l'État où le défendeur a commis une faute. En effet, eu égard à ce cas de figure, il parait plus aisé pour l'auteur de l'acte préjudiciable de choisir de commettre une atteinte dans un État où le tribunal saisi appliquera la loi du for, dans la mesure où celle-ci peut se révéler particulièrement clémente. Or le choix de la compétence du tribunal de l'État de résidence du défendeur permet d'éviter cette possibilité.

En matière de flux transfrontaliers de données à caractère personnel, la loi de l'État où le défendeur a son domicile peut être apparentée à la loi de l'État où l'entreprise est domiciliée, et de ce fait présenter les mêmes avantages et inconvénients.

C. Situation sur internet

Dans l'arrêt eDate c. Olivier Martinez, la Cour de Justice de l'Union européenne a considéré dans une affaire de diffamation sur internet que l'article 5.3 du Règlement européen

de 2001 devenu l'article 7.2) du Règlement Bruxelles 1 Bis[130] « *doit être interprété en ce sens que, en cas d'atteinte alléguée aux droits de la personnalité au moyen de contenus mis en ligne sur un site Internet, la personne qui s'estime lésée a la faculté de saisir d'une action en responsabilité, au titre de l'intégralité du dommage causé, soit les juridictions de l'État membre du lieu d'établissement de l'émetteur de ces contenus, soit les juridictions de l'État membre dans lequel se trouve le centre de ses intérêts (...) ».*[131]

Autrement dit, l'État du lieu d'établissement de l'émetteur de ces contenus revient à prendre en considération l'État du lieu du domicile de l'auteur du dommage qui sera alors compétent pour connaitre de l'ensemble du dommage.

Cet arrêt a été rendu en matière de diffamation, mais il pourrait tout à fait être applicable à un cas d'atteinte au droit de la protection des données personnelles telle que la diffusion d'une image sans le consentement de l'intéressé par voie de presse sur internet ou sur les réseaux sociaux : le tribunal compétent sera alors le tribunal de l'État dans lequel le défendeur a son domicile.

Avantages et inconvénients sur internet

Le principal avantage semble être le caractère prévisible à l'égard du défendeur à l'instance. Le seul tribunal devant lequel l'auteur du dommage pourra être attrait, sera la juridiction du lieu de son domicile principal. Dès lors, la commission de la faute par l'utilisation de la nouvelle technologie ne permet pas de remettre en cause ce facteur de rattachement puisque seul le domicile où le défendeur est établi « physiquement » sera pris en compte.

D'autre part, cela permet d'éviter que l'auteur du dommage n'ait recours à un serveur localisé dans un État étranger aux fins de commettre son acte répréhensible. En effet, le défendeur peut

---

[130] *CE, Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne :
< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF > (consulté le 27 février 2015).
[131] *Edate Advertising GmbH c. Olivier Martinez,* Affaires jointes C-509/09 et C-161/10, CJUE, 25 octobre 2011, en ligne :
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=95492 > (consulté le 6 avril 2015).

avoir recours à un serveur localisé dans un État différent que celui de son domicile principal, avec pour objectif de se faire attraire devant les juridictions de cet État.

Les inconvénients liés à ce facteur de rattachement sont exactement les mêmes que ceux étudiés précédemment hors internet.

À cet égard, le principal désavantage est le caractère injuste de cette solution à l'égard du demandeur. En effet, il parait légitime de penser que l'auteur du dommage choisisse délibérément de commettre un acte répréhensible au lieu de son domicile lorsque le tribunal de l'État, qui une fois saisi appliquera sa propre loi.

Internet ne semble pas avoir accentué, aggravé ou au contraire diminué cet inconvénient.

En matière de flux transfrontaliers de données à caractère personnel sur internet, les mêmes avantages et inconvénients peuvent être identifiés.

Cette solution est donc envisageable puisqu'elle est prévisible à l'égard de l'auteur du dommage. Toutefois, ce critère peut paraitre injuste à l'égard de la victime d'une atteinte au droit de la protection des données personnelles : le défendeur peut choisir délibérément de commettre un acte portant atteinte aux données personnelles dans son État de résidence.

Sur internet, la situation ne change pas.

Section 4. Le tribunal de l'État du domicile de la victime

A. Droit commun

En droit québécois, l'article 3141 du C.c. précité stipule que : « *Les autorités du Québec sont compétentes pour connaitre des actions personnelles à caractère extrapatrimonial et familial, lorsque l'une des personnes concernées est domiciliée au Québec* ».[132]

Une nouvelle fois, dès lors que le demandeur ou le défendeur à l'instance est domicilié au Québec, les tribunaux québécois seront compétents pour connaitre du litige.

---

[132] *Code civil du Québec*, L.Q. 1991, c.64, art. 3141.

B. Application aux données personnelles

Appliquée aux données personnelles, la situation ne semble pas revêtir de particularités : la victime d'une atteinte au droit à ses données personnelles pourra attraire le défendeur devant le tribunal du lieu où elle a son domicile.

L'application aux données personnelles en droit québécois ne semble pas poser de difficultés majeures dans la mesure où cette disposition reconnaît la compétence des tribunaux québécois en ce qui concerne les « *actions à caractère extrapatrimonial* ».[133]

Avantages et inconvénients

Ce critère de rattachement est avantageux à l'égard de la victime dans la mesure où elle n'aura pas à se déplacer dans un État autre que celui où elle a son domicile.
D'autre part, cela permet d'éluder les cas de multiplicité des recours puisque le seul tribunal compétent aux fins de trancher le litige sera le tribunal du lieu où la victime à son domicile.

Ce facteur de rattachement peut présenter un inconvénient à l'égard de l'auteur du dommage dans le cas où ce dernier n'est pas domicilié au sein de l'État où la victime est domiciliée. Toutefois, il s'agit ici avant tout de protéger la victime.

Les mêmes avantages et inconvénients peuvent être identifiés en cas de non-respect au droit de la protection des données personnelles par le biais des flux transfrontaliers.

C. Situation sur internet

Sur internet, la situation ne change pas : les mêmes avantages et inconvénients peuvent être identifiés.

L'utilisation des nouvelles technologies ne semblent pas avoir eu un impact sur ce critère de rattachement.

Ce constat vaut également pour les flux transfrontaliers de données à caractère personnel.

---

[133] *Code civil du Québec*, L.Q. 1991, c.64, art. 3141.

Cette solution est tout à fait envisageable, et cela même si elle peut présenter un inconvénient à l'encontre de l'auteur. Elle est particulièrement juste à l'égard de la victime et permet d'éviter les multiplicités de recours puisque seul sera compétent le tribunal de l'État où la victime a son domicile.

Nous allons étudier maintenant une solution spécifique qui a été développée par la Cour de Justice de l'Union européenne en matière de diffamation sur internet mais qui pourrait tout à fait être appliquée au droit de la protection des données personnelles (section 5).

Section 5. Le tribunal du centre principal des intérêts du demandeur

Il s'agit d'une solution spécifique prévue en droit de la diffamation sur internet par la Cour de Justice de l'Union européenne (A) mais qui pourrait être appliquée aux données personnelles (B). L'étude de cette solution sur internet n'est ici pas nécessaire.

A. Solution spécifique

Ce critère de rattachement ne figure pas parmi les facteurs de rattachement traditionnels puisqu'il a été mis en avant par la Cour de Justice de l'Union européenne dans le cadre d'une situation prenant place sur internet et non hors internet. Il s'agit donc de s'intéresser au droit européen, puis d'étudier les avantages et inconvénients.

Ce facteur n'est pas admis en droit commun, il s'agit uniquement d'une solution spécifique admise en matière de diffamation sur internet en droit européen.

Dans l'arrêt eDate c. Olivier Martinez,[134] la Cour de Justice de l'Union européenne a reconnu à une victime de propos diffamatoires commis sur internet, la possibilité de saisir les juridictions de l'État de sa résidence au titre de l'intégralité du dommage causé. Or, encore une fois cette solution semble tout à fait envisageable dans le cas d'atteintes au droit de la protection des données personnelles.

---

[134] *Edate Advertising GmbH c. Olivier Martinez,* Affaires jointes C-509/09 et C-161/10, CJUE, 25 octobre 2011, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=95492 > (consulté le 6 avril 2015).

La Cour souligne que « *la mise en ligne de contenus sur internet se distingue de la diffusion territorialisé d'un imprimé en ce que ceux-ci peuvent être consultés instantanément par un nombre indéfini d'internautes partout dans le monde. Ainsi, d'une part, la diffusion universelle est susceptible d'augmenter la gravité des atteintes aux droits de la personnalité et, d'autre part, de rendre extrêmement difficile la localisation des lieux de la matérialisation du dommage résultant de ces atteintes. Dans ces circonstances, étant donné que l'impact d'un contenu mis en ligne sur les droits de la personnalité d'une personne peut être mieux apprécié par la juridiction du lieu où la victime a le centre de ses intérêts (…)* ».[135]

La Cour précise que le centre d'intérêts d'une personne correspond en règle générale « *à sa résidence habituelle* ».[136]

B. Application aux données personnelles

Même si en l'espèce il s'agit de diffamation, cette solution est intéressante et pourrait tout à fait être applicable dans le cas d'atteintes au droit de la protection des données personnelles.

Avantages et inconvénients

Le principal avantage semble être le fait que ce critère permet d'éviter une multiplication des procédures : le seul tribunal compétent sera celui du lieu du centre principal des intérêts du demandeur. Or cela permet d'éluder l'imprévisibilité inhérente au choix du tribunal du lieu où le préjudice a pris place puisqu'il s'agit ici de prendre en considération, non pas une multitude de lieux où le préjudice a été subi, mais seulement le tribunal du lieu de résidence de la victime.

De plus, ce nouveau critère de rattachement semble particulièrement juste à l'égard de la victime.

---

[135] *Edate Advertising GmbH c. Olivier Martinez,* Affaires jointes C-509/09 et C-161/10, CJUE, 25 octobre 2011, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=95492 > (consulté le 6 avril 2015).
[136] *Id.*

Toutefois, ce critère de rattachement est imprévisible à l'encontre de l'auteur du dommage. D'autre part, il sera certainement attrait devant les juridictions d'un État membre autre que l'État de sa résidence principale. Dès lors, ce dernier sera contraint de se déplacer dans cet État, ce qui peut impliquer un coût financier important, ainsi qu'une perte de temps.

Cette solution est vraiment intéressante dans la mesure où elle permet d'éviter une multiplication des procédures : seul sera compétent le tribunal de l'État où le demandeur a le centre principal de ses intérêts. Il s'agit d'un critère juste et équitable à l'égard de la victime.

Toutefois, ce facteur de rattachement peut être imprévisible à l'encontre de l'auteur du dommage.

La situation ne change pas en cas d'atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers.

À présent, il s'agit de s'intéresser à d'autres facteurs de rattachement prenant place uniquement sur internet. Certains sont admis par la doctrine, d'autres non : l'accessibilité (section 6); le ciblage (section 7); le tribunal de l'État de localisation du serveur informatique (section 8); et le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires (section 9).

Les facteurs de rattachement seront présentés de manière générale (A) et ensuite appliqués aux données personnelles (B). Une étude sur internet pour chacun des critères suivants n'est pas nécessaire.

Section 6. L'accessibilité

A. Présentation générale

Ce critère se définit comme étant le fait de « *mettre le Web et ses services à la disposition de tous les individus, quelque soit leur matériel ou logiciel, leur infrastructure*

réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales ».[137]

Ce facteur de rattachement n'est pas prévu par le droit international privé québécois dans la mesure où il n'est pas considéré comme un critère de compétence juridictionnelle.

Dans un arrêt Investors Group c. Hudson,[138] la Cour Supérieure du Québec a considéré « *qu'en l'espèce, il y avait bien plus qu'un simple accès à Internet, afin de prendre compétence. A contrario, le simple accès ne semble pas suffire ».*[139]

Cependant, la Cour met en avant le fait qu'« *une activité a lieu au Québec dès qu'elle s'y manifeste, alors cette activité, si elle est considérée fautive (comme le serait l'émission de publicité sans autorisation ou sans permis de faire des affaires au Québec), déclencherait la compétence du tribunal québécois à partir d'un simple accès du site au Québec selon l'art. 3148 (3.) C.c.Q. Ainsi l'accessibilité d'un site, sans être en elle-même un critère de compétence juridictionnelle, donnerait lieu à la survenance d'une faute que l'on pourrait situer au Québec ».*[140]

Autrement dit, ce n'est pas l'accessibilité en tant que telle qui va donner compétence aux tribunaux québécois, mais le lieu de la faute ou celui du dommage.

La Cour Supérieure du Québec considère dans l'affaire National Bank of Canada c. Weir que: « *(…) based on the uncontradicted evidence, that the Postings complained of, (…) constitute « damage » which was suffered by the Bank in Québec. Until eliminated from the Website by Stockgroup, the Court is satisfied, on the balance of probabilities that the Postings were, at all relevant times, readily available and frequently consulted in Québec and elsewhere worldwide (…) ».*[141]

En l'espèce, il s'agissait d'un cas de diffamation prenant place sur internet. La Cour du Québec considère ici que les propos du défendeur ont été accessibles et consultés en ligne au

---

[137] SLOIM, E., « Pourquoi l'accessibilité numérique ? », *Openweb* (25 juillet 2005), en ligne : < http://openweb.eu.org/articles/accessibilite_numerique_pourqu > (consulté le 11 avril 2015).
[138] *Investor group c. Hudson,* [1999] R.J.Q. 599 (C.S).
[139] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*
[140] *Id.*
[141] *National Bank of Canada c. Weir,* [2010] R.J.Q. 823 (C.S).

Québec : le demandeur a donc subi un dommage sur le territoire québécois. Autrement dit, encore une fois ce n'est pas l'accessibilité en tant que telle qui donne compétence aux juridictions québécoises, mais en l'espèce la survenance du dommage au Québec.

En droit européen, dans un arrêt eDate et Olivier Martinez,[142] la Cour de Justice l'Union européenne met en avant la possibilité, pour les victimes de diffamation, de saisir « *(...) les juridictions de chaque État membre sur le territoire duquel le contenu mis en ligne est accessible ou l'a été ».*[143]

Encore une fois, la Cour ne tient pas réellement compte ici du critère de l'accessibilité en tant que tel dans la mesure où elle applique avant tout le critère de rattachement classique, à savoir la loi de l'État de survenance du dommage. Le simple fait que le contenu mis en ligne soit accessible dans un État ne peut pas suffire à admettre la compétence des juridictions de cet État, un dommage doit également y être survenu.

En droit suisse, la simple accessibilité d'un site internet ne suffit pas à engager la compétence des tribunaux suisse. Dans un arrêt du 19 juin 2009[144] en matière de droit de la consommation, la Cour de Justice de Genève a toutefois considéré que « *le fait qu'un site Internet comporte l'extension « ch. », que les prix des produits proposés à la vente sont exprimés en francs suisses, que la langue utilisée est le français et que Genève comporte indiscutablement le réservoir d'acheteurs le plus important de la Suisse francophone mène à la reconnaissance d'un for à Genève ».*[145]

---

[142] *Edate Advertising GmbH c. Olivier Martinez,* Affaires jointes C-509/09 et C-161/10, CJUE, 25 octobre 2011, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=95492 > (consulté le 6 avril 2015).
[143] *Id.*
[144] Cour de Justice de Genève, 19 juin 2009, ACJC/790/09.
[145] LALIVE AVOCATS, « Chronique de jurisprudence suisse, loi fédérale de droit international privé (LDIP) du 18 décembre 1987 (2005-2009) », (2011) 2 *Journal du droit international* 465.

De manière générale, en droit suisse, les tribunaux suisses seront déclarés compétents lorsqu'il existe un lien suffisant substantiel ou significatif entre le lieu de la faute et le territoire suisse.[146]

B. Application aux données personnelles

Il s'agit ici d'appliquer le ciblage aux données personnelles. Autrement dit, l'auteur en diffusant sur un site internet en langue allemande une photographie ou encore une adresse courriel, rend accessible ces informations au monde entier mais plus particulièrement à la population germanophone qui est plus à même de se rendre sur un site de langue allemande que la population française ou italienne par exemple.

L'accessibilité ne parait pas applicable à des situations relevant d'atteintes par le biais des flux transfrontaliers, ou du moins présenter un quelconque intérêt.

Avantages et inconvénients

Le critère de l'accessibilité présente surtout des avantages à l'égard de la victime. En effet, le demandeur à l'instance peut saisir l'ensemble des tribunaux des États où l'information est accessible.

D'autre part, cela permet à l'auteur du dommage de ne pas échapper à la justice. Le défendeur à l'instance peut avoir recours à un serveur localisé dans un État où les atteintes aux données personnelles ne sont que très faiblement sanctionnées aux fins d'éviter la compétence des tribunaux de certains États. Or le critère de l'accessibilité permet justement d'éviter cet inconvénient.

Toutefois, le simple critère de l'accessibilité ne semble pouvoir justifier la compétence d'un tribunal.

Le droit européen admet la compétence d'une juridiction d'un État membre dès lors que l'information en ligne est accessible à partir de l'un de ces États et que le dommage se matérialise au sein du même État. Le tribunal saisi ne sera alors compétent que pour connaitre

[146] LALIVE AVOCATS, « Chronique de jurisprudence suisse, loi fédérale de droit international privé (LDIP) du 18 décembre 1987 (2005-2009) », (2011) 2 *Journal du droit international* 465.

du seul dommage survenu sur le territoire. C'est donc la matérialisation du dommage au sein de l'État qui déclenche la compétence de la juridiction saisie, et non le critère de l'accessibilité seul.

De la même manière en droit québécois et en droit suisse, ce n'est pas l'accessibilité seule qui donne compétence au tribunal de l'État mais la localisation de la faute ou du dommage sur le territoire provincial.

Ainsi le critère de l'accessibilité n'a pas d'existence autonome dans la mesure où celui-ci doit coïncider avec le lieu de survenance de la faute ou celui du dommage. Cela permet finalement d'éviter les cas de « *forum shopping* » inhérents d'une certaine façon à ce facteur de rattachement.

Cette solution est intéressante mais n'a pas d'existence autonome : ce n'est pas ce critère en tant que tel qui va donner compétence aux tribunaux d'un État mais finalement le lieu de la faute ou celui du dommage. L'accessibilité conforte le choix de ce tribunal plutôt qu'un autre mais ne peut en aucun cas donner la compétence à un tribunal de manière autonome car cela pourrait avoir pour effet la multiplicité des fors compétents : les tribunaux du monde entier pourraient alors se déclarer compétents dans la mesure où le site est accessible sur leur territoire.

Section 7. Le ciblage

A. Présentation générale

Il s'agit avant tout de définir le critère du ciblage qui correspond au fait de « *prendre en compte l'impact de l'activité ou le lieu vers lequel elle est dirigée* ».[147]

[147] TURK, A., *La vie privée en péril : Des citoyens sous contrôle*, coll. « OJ.SC. Humaines », Paris, éd. Odile Jacob Broché, 2011.

Le critère du ciblage ou la théorie de la focalisation a d'abord été développé par la jurisprudence américaine et a été notamment repris par la Cour de Justice de l'Union européenne dans une affaire Hotel Apenhof. [148] Cette théorie reprend finalement le critère de l'accessiblité en y ajoutant un faisceau d'indices nécessaires pour fonder la compétence d'un tribunal.

Le droit international privé québécois ne prévoit pas le critère du ciblage. D'après le Professeur en droit international privé à l'Université de Montréal, Monsieur Gérald Goldstein : « *la détermination de la compétence québécoise est indépendante d'un tel critère, même si la prévisibilité imprègne l'art. 3148 et notamment le rattachement fondé sur le fait qu'une obligation devait être exécutée au Québec ».*[149]

En droit européen, le critère du ciblage est « *déjà utilisé dans le domaine du droit de la consommation ».*[150]

Dans l'affaire Hotel Apenhof [151], la Cour de Justice considère que la simple accessibilité du site sur le territoire d'un État membre ne suffit pas à fonder la compétence des tribunaux de cet État, et qu'un ensemble de critères doivent être pris en compte par les juridictions nationales aux fins de déterminer si il y a une volonté ou non de la part du demandeur de diriger son activité vers un État en particulier. Parmi ces critères, nous pouvons citer : « *(...) la nature internationale de l'activité, la mention d'itinéraires à partir d'autres États membres pour se rendre au lieu où le commerçant est établi, l'utilisation d'une langue ou d'une monnaie autres que la langue ou la monnaie habituellement utilisées dans l'État membre dans lequel est établi le commerçant avec la possibilité de réserver et de confirmer la réservation dans cette autre langue, la mention de coordonnées téléphoniques avec l'indication d'un préfixe international, l'engagement de dépenses dans un service de référencement sur Internet afin de faciliter aux consommateurs domiciliés dans d'autres États membres l'accès au site du*

---

[148] *Hôtel Apenhof c. Oliver Heller,* Affaire C-144/09, 7 décembre 2010, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=96720 > (consulté le 7 avril 2015).
[149] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*
[150] *Id.*
[151] *Hôtel Apenhof c. Oliver Heller,* Affaire C-144/09, 7 décembre 2010, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=96720 > (consulté le 7 avril 2015).

commerçant ou à celui de son intermédiaire, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État membre où le commerçant est établi et la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres (…) ».[152]

B. Application aux données personnelles

Pour reprendre l'exemple précédent concernant l'auteur d'un dommage qui publie sur un site allemand le nom, le prénom ou encore une photographie d'une personne, ici, la simple accessibilité par la population germanophone ne suffit pas : il faut l'intention de la part de l'auteur de cibler cet État, c'est-à-dire l'État allemand et non un autre État. Comment cela peut-il se matérialiser en matière d'atteintes au droit de la protection des données personnelles? Cette question est ici compliquée en ce qui concerne les données personnelles contrairement au droit de la consommation où la langue, la devise utilisée afin de payer les produits achetés ou encore les lieux de livraison dans un État en particulier peuvent permettre d'établir que l'auteur a voulu cibler tel État plutôt qu'un autre.

La situation étant différente en matière d'atteintes au droit de la protection des données personnelles, quels sont les éléments qui pourraient être pris en compte afin de considérer que l'auteur a voulu cibler cet État en particulier ?

Nous pouvons imaginer que la publication sur un site germanophone, qui est donc écrit en allemand, des nom et prénom ou autres éléments d'identification personnel d'une personne de nationalité allemande, domiciliée en Allemagne permettent d'établir que l'auteur a voulu cibler l'Allemagne et non un autre État. D'autre part, nous pouvons regarder les commentaires du site et regarder si ceux-ci sont rédigés en langue allemande : des commentaires rédigés en plusieurs langues indiqueraient un site d'envergure internationale et non spécifiquement destiné à la population germanophone.

---

[152] *Hôtel Apenhof c. Oliver Heller,* Affaire C-144/09, 7 décembre 2010, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=96720 > (consulté le 7 avril 2015).

De la même manière, le ciblage ne semble pas applicable en cas d'atteintes aux flux transfrontaliers de données à caractère personnel.

Avantages et inconvénients

Le principal avantage semble être le respect du principe de prévisibilité de ce facteur de rattachement à l'égard du défendeur à l'instance. En effet, en ciblant particulièrement un État, il émane de la part de l'auteur du dommage une volonté de porter préjudice à la victime au sein de cet État membre pouvant s'apparenter au lieu de la résidence principale de cette dernière.

En ce qui concerne les données personnelles, l'utilisation du ciblage est difficile dans la mesure où les éléments susceptibles de constituer des indices permettant d'établir la volonté du défendeur de cibler tel État plutôt qu'un autre sont difficilement identifiables. Ceux cités précédemment, à savoir l'État de domiciliation de la victime ou la langue du site internet ne semblent pas suffisants pour établir cette volonté. Dès lors, il semble que le ciblage ne puisse être utilisé que pour conforter le choix d'un critère : le tribunal de l'État de survenance de la faute ou du préjudice par exemple.

Cette solution est intéressante dans la mesure où elle est prévisible à l'égard du défendeur. Toutefois, ce critère est difficilement applicable en ce qui concerne le droit à la protection des données personnelles dans la mesure où les éléments permettant d'établir la volonté de l'auteur du dommage de cibler un État en particulier sont difficiles à établir.

Section 8. Le tribunal de l'État de localisation du serveur informatique

A. Présentation générale

Ce critère de rattachement n'a été considéré par aucun des systèmes juridiques étudiés. À cet égard, les juridictions québécoises ont définitivement écarté ce facteur de rattachement.

Le serveur informatique offre aux internautes différentes prestations tels que la messagerie ou courriel ou encore le stockage de certaines données par exemple.

Dans un arrêt Investor group c. Hudson,[153] la Cour supérieure de Montréal a eu à se prononcer sur un litige en matière de diffamation sur internet. En l'espèce, il s'agissait d'une personne domiciliée au Québec, et qui à l'aide d'un serveur localisé aux États-Unis avait tenu des propos diffamatoires à l'égard d'une société québécoise. Le tribunal québécois s'est déclaré compétent pour connaitre du litige dans la mesure où le préjudice était localisé au Québec, et le simple fait que l'auteur des propos diffamatoires ait utilisé un serveur américain n'avait ici aucune importance.

B. Application aux données personnelles

Le tribunal compétent sera celui de l'État où est localisé le serveur informatique de la personne ayant diffusé des informations personnelles sur un site internet. Appliqué aux données personnelles, ce facteur de rattachement ne semble pas revêtir de caractéristiques particulières.

Avantages et inconvénients

Le principal avantage à ce critère de rattachement semble être la prévisibilité que cela implique à l'égard du défendeur. Ce dernier ne sera dès lors pas attrait devant une multitude de juridictions puisque seul sera pris en considération, le tribunal du lieu où le serveur informatique est localisé.

Cependant, le tribunal du lieu de localisation du serveur informatique présente de nombreux inconvénients, et cela notamment à l'égard de la victime.

Le principal désavantage demeure le caractère injuste et inéquitable du recours à ce critère. En effet, il parait dès lors possible pour le défendeur à l'instance d'avoir recours à un serveur informatique établi dans un État ayant des lois clémentes en matière d'atteintes à la vie privée et aux données personnelles, et ainsi se soustraire aux tribunaux du lieu de son État de résidence. Cela peut avoir pour effet de léser de manière significative la victime.

---

[153] *Investor group c. Hudson,* [1999] R.J.Q. 599 (C.S).

D'autre part, de quelle façon est-il possible de matérialiser physiquement le lieu du serveur informatique ? En effet, localiser un serveur peut se révéler selon les circonstances extrêmement difficile.

Enfin, il convient de souligner que le serveur n'a pas de lien direct avec le droit dans la mesure où il s'agit d'une machine donc l'envisager en tant que critère de rattachement ne semble pas pertinent. En d'autres termes, il n'y aura pas de liens suffisants entre le tribunal de l'État et le litige en cause.

En ce qui concerne les flux transfrontaliers, aucune spécificité n'est ici à relever.

Cette solution n'est absolument pas envisageable en raison de son caractère profondément arbitraire et injuste qu'elle revêt à l'égard de la victime de l'atteinte au droit de la protection des données personnelles. D'autre part, encore une fois le serveur n'a aucun lien direct avec le droit et de ce fait ne peut être envisagé comme un critère de rattachement.

Section 9. Le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires

A. Présentation générale

Cette solution consisterait à prendre en compte le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires. Qu'est-ce que cela signifie ?

Le fournisseur d'accès est l'entreprise en charge d'offrir aux internautes une connexion à internet (par exemple *Vidéotron* au Québec), et l'hébergeur et/ou les intermédiaires est l'acteur qui héberge des sites internet, c'est-à-dire l'intermédiaire technique entre une entreprise et les internautes (par exemple *Amazon*).

B. Application aux données personnelles

Une entreprise domiciliée dans un État européen diffuse sur son site internet la photographie ou certaines informations personnelles concernant un individu : le site où les propos litigieux sont diffusés, est hébergé par *Google*. Ce seront donc les juridictions américaines et plus particulièrement californiennes qui seront compétentes.

De la même manière en ce qui concerne le fournisseur d'accès à internet : le tribunal compétent sera la juridiction de l'État où est localisé le fournisseur d'accès à internet. Une entreprise ou une personne domiciliée au Québec diffusant des informations personnelles sur un individu, et qui utilise pour ce faire le fournisseur d'accès *Vidéotron* : le tribunal compétent sera alors le tribunal québécois. Il parait important de noter que finalement le tribunal de l'État du fournisseur d'accès revient à prendre en compte le tribunal de l'État où le défendeur est domicilié puisqu'il sera possible de prendre une connexion *Vidéotron* par exemple que si nous sommes directement domiciliés sur le territoire québécois.

Avantages et inconvénients

Le principal avantage semble être l'aspect prévisible à l'égard du défendeur à l'instance. En effet, le seul tribunal compétent sera le tribunal de l'État où se trouve le fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires.

Le principal inconvénient semble être le caractère inéquitable à l'égard de la victime. En effet, l'auteur du dommage peut utiliser un fournisseur d'accès à internet ou un hébergeur localisé dans un État ne sanctionnant que très faiblement les atteintes au du droit à la protection des données personnelles, et cela aux fins d'éviter la législation de son État de résidence par exemple.

D'autre part, de quelle façon est-il possible de localiser l'hébergeur ou le fournisseur d'accès à internet ? À cet égard, cette interrogation conserve toute son importance dans le cas des utilisateurs des réseaux *Tor* ou autres réseaux anonymes, dans la mesure où ces derniers arrivent par un mélange de réseaux à effacer leurs données de navigation et donc leurs traces sur la toile.[154] Or la difficulté liée à la localisation d'un fournisseur d'accès ou de toute connexion rend impossible pour un tribunal de reconnaitre sa compétence.

De plus, dans le cas de l'hébergeur internet, ce dernier a pour principale activité de mettre à disposition des internautes des serveurs. À cet égard, de quelle manière est-il possible de localiser l'hébergeur ? S'agit-il de prendre en compte la localisation de l'ensemble des

[154] Wikipédia Encyclopédie libre, « Tor (réseau) », *Wikipédia* (23 avril 2015), en ligne : < http://fr.wikipedia.org/wiki/Tor_%28r%C3%A9seau%29 > (consulté le 10 mai 2015).

serveurs mis en place ? Cette possibilité n'aura-t-elle pas pour effet d'entrainer une multiplicité des procédures ?

De ce fait, convient-il de prendre en considération la localisation de l'hébergeur ? Cependant, de quelle façon une nouvelle fois est-il possible de localiser l'hébergeur ?

Enfin, cette solution ne semble pas présenter d'intérêts particuliers et est injuste à l'égard de la victime.

La situation ne change pas pour les atteintes au droit à la protection des données personnelles par le biais des flux transfrontaliers.

Cette solution n'est absolument pas envisageable : elle ne présente aucun intérêt particulier et est injuste à l'égard de la victime.

Il convient à présent de s'intéresser à une solution qui n'est pas en tant que telle un critère de rattachement : le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige, le forum « *non conveniens* » (section 10).

Section 10. Le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige : le forum « *non conveniens* »

A. Droit commun

La théorie du forum « *non conveniens* », qui se retrouve en droit québécois, est : « *(...) l'affirmation du pouvoir discrétionnaire qui est reconnu aux juges, dans les pays de Common Law, de ne pas exercer leur compétence internationale à l'égard d'un litige qui relève pourtant de leur pouvoir juridictionnel, dès lors qu'ils estiment qu'il serait plus opportun qu'il soit tranché par un for étranger également compétent* ».[155]

[155] MERCADAL, B., « Règle dite du « Forum non conveniens » dans les pays de Common Law », *Institut international de Droit et d'Expression et d'inspiration Françaises* (21 février 2005), en ligne :

En droit québécois, l'article 3135 du C.c.Q dispose que : « *Bien qu'elle soit compétente pour connaitre d'un litige, une autorité du Québec peut, exceptionnellement et à la demande d'une partie, décliner cette compétence si elle estime que les autorités d'un autre État sont mieux à même de trancher le litige* ».

La théorie du forum « *non conveniens* » prévu par l'article 3135 du C.c.Q a fait l'objet de multiples études doctrinales,[156] et certains auteurs ont mis en avant que son introduction en droit québécois a posé de nombreux problèmes quant à son application : « *(…) les plaideurs l'invoquent fréquemment et (…) les magistrats ont de la difficulté à en établir les balises* ».[157]

Dans un arrêt Oppenheim forfait GMBH c. Lexus maritime inc.,[158] la Cour d'appel du Québec a établi une liste de facteurs à prendre en considération afin, pour un tribunal, d'affirmer ou d'infirmer sa compétence : « *Le juge saisi d'un moyen déclinatoire doit considérer plusieurs facteurs afin de déterminer s'il est en présence d'une situation exceptionnelle. Au cours des dernières années, les tribunaux ont précisé le sens et la portée de l'article 3135 du C.c.Q. Les critères à considérer comprennent, entre autres : 1) le lieu de résidence des parties et des témoins ordinaires et experts; 2) la situation des éléments de preuve; 3) le lieu de formation et d'exécution du contrat qui donne lieu à la demande; 4) l'existence et le contenu d'une autre action intentée à l'étranger et le progrès déjà effectué dans la poursuite de cette action; 5) la situation des biens appartenant au défendeur; 6) la loi applicable au litige; 7) l'avantage dont*

< http://www.institut-idef.org/Regle-dite-du-Forum-non-conveniens.html > (consulté le 4 avril 2015).

[156] GLENN, H.P., «Droit international privé», dans *La réforme du Code civil*, Barreau du Québec et Chambre des Notaires du Québec, P.U.L., Sainte-Foy, 1993, 669, n° 73; TALPIS, J.A., et CASTEL, J.-G, «Le Code civil du Québec — Interprétation des règles de droit privé» dans *La Réforme du Code civil*, t. 3, Québec, Presses de l'Université Laval, 1993, 902, n° 411 et s.; GOLDSTEIN, G., «Chap. Canada (Québec)», *in Declining Jurisdiction in Private International Law*, par J.J. Fawcett (éd.), Oxford, Clarendon Press, 1995, 146-157; GOLDSTEIN, G., et GROFFIER, E., *Traité de droit civil. Droit international privé*, vol. 1, *Théorie générale*, Cowansville, éd. Yvon Blais, 1998, n° 134 ; SAUMIER, G., «*Forum non conveniens*, Where are we now?», (2000) 12 *S.C.L.R.* (2d) 121; TALPIS, J.A, et KATH, S. L., «The Exceptional as Commonplace in Quebec *Forum non conveniens* Law: *Cambior*, a case in Point», (2000) 34 *R.J.T.* 761 ; SAUMIER, G., «Le *forum non conveniens* au Québec: bilan d'une transplantation», dans *Mélanges en l'honneur du professeur Alain Prijuner*, par S. Guillemard (dir.), Thomson Reuters Canada, 2011, 345 ; LEBEL, L., et CHABOT, G., «L'essai d'un mariage : l'intégration du forum non conveniens dans le droit international privé québécois», dans *Mélanges en l'honneur du professeur Alain Prujiner*, par S. Guillemard (dir.), Thomson Reuters Canada, 2011, 267 ; EMANUELLI, C., *Droit international privé québécois*, 3ème éd. Wilson & Lafleur, 2011, n° 164-167 ; SABOURIN, F., «Motifs permettant de ne pas exercer la compétence : *forum non conveniens* et litispendance internationale», fascicule 9, dans *JurisClasseur Québec*, volume *Droit international privé*, LexisNexis, feuilles mobiles ; GOLDSTEIN, G., *Commentaires sur le Code civil du Québec, Droit international privé, vol. 2, Compétence internationale des autorités québécoises et effets des décisions étrangères (art. 3134 à 3168 C.c.Q.)*, éd. Yvon Blais, 2013, n° 3135-500 à 3135-590.

[157] GUILLEMARD, S., PRUJINER, A., SABOURIN, F., « Les difficultés de l'introduction du *forum non conveniens* en droit québécois », (1995) 36 *C. de D.* 91; et voir aussi GUILLEMARD, S., et TÊTE, M., « Le forum non conveniens au Québec, une vingtaine d'années plus tard : encore quelques questions non résolues », (2012) 25.1 *Revue québécoise de droit international* 175.

[158] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).

jouit la demanderesse dans le for choisi; 8) l'intérêt de la justice; 9) l'intérêt des deux parties; 10) la nécessité éventuelle d'une procédure en exemplification à l'étranger ».[159]

En droit suisse, l'article 3 de la loi fédérale dispose que : « *Lorsque la présente loi ne prévoit aucun for en Suisse et qu'une procédure à l'étranger se révèle impossible ou qu'on ne peut raisonnablement exiger qu'elle y soit introduite, les autorités judiciaires ou administratives suisses avec lequel la cause présente un lien suffisant sont compétentes ».*[160]

En d'autres termes, les tribunaux suisses seront compétents dès lors que le litige en cause présente des liens suffisants avec les autorités judiciaires suisses.

Cela revient finalement à prendre en compte le tribunal de l'État le plus compétent pour trancher le litige.

B. Application aux données personnelles

Eu égard à la liste établie par la Cour d'appel du Québec dans l'arrêt Oppenheim forfait GMBH c. Lexus maritime inc,[161] quels critères sont susceptibles de s'appliquer aux données personnelles ?

Nous allons développer les critères développés par la Cour d'appel du Québec et les appliquer aux données personnelles.

Il y a cinq critères qui paraissent pertinents appliqués aux données personnelles, à savoir : le « *lieu de résidence des parties et des témoins ordinaires et experts* »,[162] l'« *existence et le contenu d'une autre action intentée à l'étranger et le progrès déjà effectué dans la poursuite de cette action »,*[163] l'« *avantage dont jouit la demanderesse dans le for choisi* »,[164] l'« *intérêt de la justice* »[165] et l'« *intérêt des deux* parties ».[166]

---

[159] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[160] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art.3.
[161] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Id.*
[166] *Id.*

Le « *lieu de résidence des parties et des témoins ordinaires et experts* »[167] est intéressant dans la mesure où le choix de ce critère présente des liens suffisants avec le litige, et est parfaitement applicable aux cas d'atteintes au droit de la protection des données personnelles.

L'« *existence et le contenu d'une autre action intentée à l'étranger et le progrès déjà effectué dans la poursuite de cette action »*[168] est un critère intéressant en cas de violation des données personnelles. En effet, le dommage peut être subi dans de nombreux États notamment en cas d'atteintes au droit à la protection des données personnelles. Or, dans le cas où plusieurs tribunaux sont saisis du même litige, le déclinement de compétence d'une juridiction saisi en raison d'une action déjà intentée dans un autre État, peut permettre d'éviter une pluralité de procédure.

L' « *avantage dont jouit la demanderesse dans le for choisi* »[169] pourrait également être un critère à prendre en compte en cas d'atteintes aux données personnelles : il convient de donner préséance au choix effectué par la partie demanderesse qui a décidé d'attraire la partie défenderesse devant les tribunaux québécois, sauf si ce choix n'a pas pour effet de l'avantager.

L'« *intérêt de la justice* »[170] combiné avec l'« *intérêt des deux* parties » sont des critères pouvant présenter des liens suffisants avec le litige, et sont justes et équitables.

D'autres éléments paraissent pertinents : la « *situation des éléments de preuve* »,[171] la « *situation des biens appartenant au défendeur* »,[172] ou encore la « *nécessité éventuelle d'une procédure en exemplification à l'étranger* ».[173]

La « *situation des éléments de preuve* »[174] peut avoir une certaine proximité avec le litige et pourrait effectivement s'appliquer dans le cas d'un litige impliquant une violation du droit à la protection des données personnelles.

---

[167] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[168] *Id.*
[169] *Id.*.
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] *Id.*

La « *situation des biens appartenant au défendeur* »[175] peut être pertinente en matière d'atteintes au droit de la protection des données personnelles. En effet, lorsque le tribunal saisi est le tribunal de l'État où la faute a été commise mais que celui ne correspond pas à l'État du domicile du défendeur ou plus généralement de l'État où l'ensemble de ses biens sont situés, le tribunal de l'État de la faute peut n'avoir aucun lien suffisant avec le litige en cause.

La *« nécessité éventuelle d'une procédure en exemplification à l'étranger »*[176] peut également être pris en compte.

Deux autres critères ne semblent pas être pertinents appliqués aux données personnelles, à savoir : le « *lieu de formation et d'exécution du contrat qui donne lieu à la demande »*[177] et la « *loi applicable au litige* ».[178]

Le « *lieu de formation et d'exécution du contrat qui donne lieu à la demande »*[179] n'est ici pas applicable à un litige relevant de la matière extracontractuelle/délictuelle telle qu'une atteinte au droit de la protection des données personnelles.

La « *loi applicable au litige* »[180] n'est pas pertinente lorsqu'il s'agit d'un litige impliquant une atteinte au droit de la protection des données personnelles dans la mesure où il est question de responsabilité civile extracontractuelle/délictuelle, et non contractuelle. Il n'y a pas de désignation de la loi applicable, comme cela peut être le cas dans un contrat où les parties choisissent la loi qui sera applicable en cas de litige.

Autrement dit, l'ensemble des éléments établis par la Cour du Québec dans l'arrêt Oppenheim forfait GMBH c. Lexus maritime inc.,[181] peuvent être appliqués en cas d'atteintes au droit à la protection des données personnelles. Il s'agit finalement d'éléments assez généraux pouvant s'appliquer à un nombre important de litiges.

---

[175] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.*.

Seuls deux éléments ne semblent absolument pas pertinents, le lieu de la formation du contrat et la loi qui est applicable au litige dans la mesure où il s'agit d'éléments s'appliquant davantage à un litige relevant de la responsabilité civile contractuelle.

En matière d'atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers, les mêmes critères peuvent être mis en avant.

Avantages et inconvénients

Le déclinement de compétence d'un tribunal au profit d'un autre tribunal jugé plus à même de trancher le litige, permet d'éviter les cas de multiplicité des recours. En effet, si le demandeur à l'espèce choisit de saisir deux ou plusieurs juridictions différentes, cela peut avoir pour effet de porter préjudice au défendeur à l'action. La multiplicité des recours intentés est possible dans la mesure où le préjudice subi par la victime en matière d'atteintes au droit de la protection des données personnelles peut se matérialiser dans différents États.

Or cette multiplicité présente plusieurs inconvénients : la saisie de plusieurs tribunaux peut constituer un coût important à l'égard du demandeur et du défendeur à l'instance et également une différence d'appréciation selon les tribunaux, c'est-à-dire une possibilité que des jugements contradictoires soient rendus.

Cependant, le déclinement de compétence d'un tribunal au profit d'un autre tribunal considéré comme plus enclin à trancher le litige, présente un inconvénient majeur à l'égard du défendeur.

En effet, le forum « *non conveniens* » peut s'avérer préjudiciable dans la mesure où cela risque de porter atteinte au principe de prévisibilité à l'égard du défendeur à l'instance. En effet, le défendeur peut légitimement s'attendre à être attrait devant le tribunal initialement saisi.

La situation ne change pas pour les atteintes au droit à la protection des données personnelles par le biais des flux transfrontaliers.

C. Situation sur internet

D'autres éléments spécifiques à internet dans le cas où il s'agit de la diffusion d'éléments personnels sur un site, pourraient être pris en compte : la langue de diffusion du

site internet et également la langue de rédaction des commentaires des internautes, s'il y en a. Ces critères, associés à d'autres critères de la jurisprudence Oppenheim forfait GMBH c. Lexus maritime inc,[182]pourraient permettre au tribunal d'infirmer ou d'affirmer sa compétence en cas d'atteintes au droit de la protection des données personnelles sur internet.

En matière de flux transfrontaliers de données à caractère personnel, les mêmes critères qu'hors internet peuvent être pris en compte.

Le « *forum non conveniens* » pourrait être appliquée à un litige relatif aux données personnelles. Cette théorie a de nombreux avantages, notamment pour éviter la pluralité de tribunaux saisis puisque le tribunal pourra choisir d'infirmer sa compétence au regard de « *l'existence et le contenu d'une autre action intentée à l'étranger et le progrès déjà effectué dans la poursuite de cette action* ».[183] Toutefois, cette solution présente un caractère d'imprévisibilité à l'égard de l'auteur du dommage.

[182] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[183] *Id.*

Synthèse

Certaines solutions sont intéressantes et envisageables malgré les inconvénients qu'elles présentent, d'autres pourraient être envisageables mais ne présentent pas véritablement d'existence autonome ou ne paraissent pas pouvoir s'appliquer aux données personnelles, et enfin certaines ne le sont absolument pas.

En ce qui concerne les solutions envisageables, nous retrouvons celles de droit commun à savoir le tribunal de l'État du préjudice, le tribunal de l'État de la faute, le tribunal de l'État du domicile du défendeur ou encore le tribunal de l'État du domicile de la victime.

Parmi ces solutions, certaines sont davantage favorables à la victime tels que le tribunal de l'État du préjudice et le tribunal de l'État du domicile de la victime. D'autres sont favorables à l'égard de l'auteur du dommage, à savoir le tribunal de l'État de la faute et le tribunal de l'État du domicile du défendeur.

Le tribunal de l'État du préjudice prévu en droit québécois, en droit européen et en droit suisse, est une solution envisageable dans la mesure où elle est juste et équitable à l'égard de la victime. Cependant, ce critère demeure imprévisible à l'encontre de l'auteur du dommage dans la mesure où le préjudice peut être subi dans différents lieux par la victime.

D'autre part, sur internet les inconvénients peuvent être accentués puisqu'une atteinte au droit des données personnelles peut être localisée dans de nombreux États.

Le tribunal de l'État du domicile de la victime, mis notamment en avant en droit québécois, est profondément juste et équitable à l'égard de la victime d'une part, et permet d'autre part, d'éviter les cas de multiplicité de fors compétents puisque seul sera compétent le tribunal de l'État du domicile de la victime. Cependant, cette solution peut paraitre injuste à l'encontre de l'auteur du dommage qui pourra être contraint de se déplacer dans un État autre que celui où il a son domicile.

Internet n'a ici aucune conséquence sur ce critère de rattachement.

Le tribunal de l'État où la faute a été commise, prévu en droit québécois, en droit européen et en droit suisse, respecte le principe de prévisibilité à l'égard de l'auteur du dommage. Toutefois, ce facteur est injuste envers la victime : le défendeur pouvant choisir de commettre

une faute dans un État en fonction de la loi que le tribunal de cet État une fois saisi, appliquera.

Sur internet, la situation ne change pas véritablement.

Le tribunal de l'État du domicile du défendeur, également prévu en droit québécois, en droit européen et en droit suisse, présente un aspect prévisible à l'égard de l'auteur du dommage. Cependant, une telle solution peut être injuste à l'égard de la victime dans la mesure où le défendeur à l'instance peut choisir délibérément de commettre un acte portant atteinte au droit de la protection des données personnelles dans son État de résidence en fonction de la loi que le tribunal saisi appliquera.

À nouveau, sur internet la situation ne semble pas revêtir de particularités.

Uniquement appliquée à internet, une solution, notamment envisagée en droit européen, parait intéressante et envisageable : le tribunal du centre principal des intérêts du demandeur.

Ce critère permet d'éviter une multiplication des procédures puisque seul sera compétent le tribunal de l'État où le demandeur a le centre principal de ses intérêts. D'autre part, il est particulièrement juste et équitable à l'égard de la victime. Toutefois, ce facteur de rattachement peut être imprévisible à l'encontre de l'auteur du dommage.

D'autres solutions envisagées par la doctrine sont intéressantes mais pas nécessairement envisageables : le critère de l'accessibilité et celui du ciblage.

L'accessibilité, bien qu'intéressante également, n'a pas d'existence autonome : ce n'est pas ce critère en tant que tel qui va donner compétence aux tribunaux d'un État mais finalement le lieu de la faute ou le lieu du préjudice. Ce facteur appuie la compétence du tribunal de l'État plutôt qu'un autre.

Le ciblage est une solution prévisible envers le défendeur. Cependant, ce facteur de rattachement est difficilement applicable en ce qui concerne le droit à la protection des données personnelles dans la mesure où les critères permettant d'établir la volonté de l'auteur du dommage de cibler un État en particulier sont difficiles à établir.

Le critère du ciblage peut donc servir à conforter le choix de la compétence du tribunal de l'État de la faute ou du dommage par exemple.

Certaines solutions, également prévues ou non par la doctrine, ne sont absolument pas envisageables : le tribunal de l'État de localisation du serveur informatique et le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires.

Le tribunal de l'État de localisation du serveur informatique n'est absolument pas envisageable en raison de son caractère profondément arbitraire et injuste qu'elle revêt à l'égard de la victime de l'atteinte aux données personnelles. D'autre part, encore une fois le serveur n'a aucun lien direct avec le droit et de ce fait ne peut être envisagé comme un critère de rattachement.

Le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires n'est pas une solution envisageable car elle ne présente aucun intérêt particulier avec le litige et est injuste à l'égard de la victime.

Enfin, une solution, bien qu'il ne s'agisse pas d'un critère en tant que tel, mérite d'être mentionnée : le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige, le forum « *non conveniens* ».

Le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige, le forum « *non conveniens* » prévu en droit pourrait être appliqué à un litige relatif aux données personnelles : cela peut permettre d'éviter la pluralité de tribunaux saisis puisque le tribunal pourra choisir d'infirmer sa compétence au regard de certains éléments mentionnés par la Cour du Québec dans l'arrêt Oppenheim forfait GMBH c. Lexus maritime inc.[184]

Sur internet, d'autres éléments pourraient être envisagés, tel que la langue utilisée sur le site internet, ou encore la langue de rédaction des commentaires des internautes.

Cependant, la théorie du « *forum non conveniens* » présente une grande imprévisibilité à l'encontre de l'auteur du dommage.

---

[184] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).

Il convient à présent d'étudier les données personnelles et les conflits de lois (Chapitre 2). À cet égard, certaines solutions envisagées dans le cadre du Chapitre 1 seront à nouveau analysées au regard non plus de la compétence juridictionnelle, mais des conflits de lois. Encore une fois, certains de ces critères sont prévus en droit commun, d'autres par la doctrine. D'autre part, de nouveaux facteurs de rattachement prévus par le droit commun ou la doctrine vont être étudiés. À contrario, certains critères prévus ou non par la doctrine seront définitivement écartés dans ce nouveau chapitre, et notamment le critère donnant compétence au tribunal de l'État de la localisation du serveur informatique qui ne revêt aucun intérêt.

Chapitre 2 : Données personnelles et conflits de lois

Après avoir étudié la compétence des tribunaux au regard des systèmes juridiques québécois, européen et suisse, il convient à présent de s'intéresser aux données personnelles et conflits de lois : une fois le tribunal compétent saisi, quelle loi va-t-il appliquer ?

Plusieurs facteurs de rattachement peuvent être mis en avant, à savoir : la loi de l'État du préjudice (section 1), la loi de l'État de la faute (section 2), la loi de l'État de résidence ou du domicile du demandeur et du défendeur à l'instance (section 3), et la loi de l'État de la résidence habituelle du défendeur à l'instance (section 4).

Pour chacun de ces critères, et de la même façon que dans le cadre du chapitre 1, le droit commun (A), l'application aux données personnelles (B) puis la situation sur internet (C) seront envisagés. Encore une fois, les avantages et inconvénients pour chaque facteur seront étudiés hors puis sur internet, le cas échéant.

D'autre part, la loi de l'État favorisant la victime (section 5) peut également être énoncée. Il s'agit ici d'une disposition particulière (A), que nous allons appliquer aux données personnelles (B) puis également étudier sur internet (C). De la même manière, les avantages et inconvénients hors puis sur internet seront analysés le cas échéant.

Enfin d'autres critères de rattachement, qui ne relèvent pas du droit commun mais sont admis ou pas par la doctrine peuvent être présentés, tels que : l'accessibilité (section 6), le ciblage (section 7), la loi de l'État du fournisseur d'accès à internet de l'hébergeur et/ou des intermédiaires (section 8), la loi de l'État « offrant la meilleure protection des données à caractère personnel » (section 9), la loi de l'État où est établi le « *maître du fichier* »[185] (section 10).

Selon les critères de rattachement envisagés, une présentation générale sera faite lorsque davantage d'éclaircissements doivent être apportés dans le cadre des conflits de lois (A), et l'application aux données personnelles étudiée pour chaque facteur (B). À nouveau, puisqu'il

---

[185] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.

est ici question de facteurs de rattachement prenant place uniquement sur internet, l'application du critère à une situation prenant place sur internet n'est pas nécessaire.

Section 1. La loi du lieu du préjudice

A. Droit commun

En droit québécois, l'article 3126 du C.c.Q applicable en matière de responsabilité civile dispose que : « *L'obligation de réparer le préjudice causé à autrui est régie par la loi de l'État où le fait générateur du préjudice est survenu. Toutefois, si le préjudice est apparu dans un autre État, la loi de cet État s'applique si l'auteur devait prévoir que le préjudice s'y manifesterait* ».[186]

En d'autres termes, la loi du lieu du préjudice ne sera applicable que lorsque celle-ci diffère de la loi du lieu de survenance de la faute et que cela est prévisible pour l'auteur du dommage.

En droit européen, il parait opportun de préciser que le Règlement Rome II applicable aux obligations non contractuelles a exclu de son champ d'application les atteintes relatives à la vie privée et à la diffamation, et plus généralement aux données personnelles. À cet égard, l'article 1g) dispose que sont exclues : « *Les obligations non contractuelles découlant d'atteintes à la vie privée et aux droits de la personnalité, y compris la diffamation* ».[187]

Cependant, le Parlement européen a émis une proposition de modification du Règlement dans lequel les droits relatifs à la vie privée seraient inclus. Le nouvel article 5 bis alinéa 1 stipule que : « *La loi applicable à une obligation non contractuelle résultant d'une atteinte à la vie privée ou aux droits de la personnalité, y compris la diffamation, est celle du pays où se produisent ou sont susceptibles de se produire le ou les éléments les plus significatifs de la perte ou du dommage* ».[188]

---

[186] *Code civil du Québec,* L.Q., 1991, c. 64, art.3126.
[187] CE, *Règlement (CE) n. 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »),* 2007, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32007R0864&from=FR > (consulté le 7 mars 2015).
[188] CE, *Proposition de recommandations détaillées concernant le Règlement (CE) n°864/2007 sur la loi applicable aux obligations non contractuelles (Rome II) (2012).*

Et l'alinéa 2 de poursuivre : « *Toutefois, la loi applicable est la loi du pays dans lequel le défendeur a sa résidence habituelle si celui-ci ne pouvait pas avoir raisonnablement prévu les conséquences importantes de son acte dans le pays désigné par le paragraphe 1 ».*[189]

En d'autres termes, la loi applicable sera la loi de l'État où l'élément le plus significatif du dommage a été subi dans le cas où le défendeur pouvait prévoir que ce serait la loi de cet État qui serait applicable. Dans le cas contraire, la loi applicable sera la loi de l'État où ce dernier a sa résidence habituelle.

En droit suisse, l'article 133 al.2 de la loi fédérale sur le droit international privé dispose que : « *(...) Toutefois, si le résultat s'est produit dans un autre État, le droit de cet État est applicable si l'auteur devait prévoir que le résultat s'y produirait ».*[190]

Autrement dit, la loi de l'État où le préjudice est survenu est applicable dans le cas où le défendeur à l'instance pouvait légitimement s'attendre à ce que le dommage se produirait au sein de cet État : il y a donc une condition de prévisibilité quant à l'application de la loi de l'État où le préjudice est survenu.

B. Application aux données personnelles

Une personne porte atteinte au droit à l'image d'une personne ou diffuse certains de ses éléments personnels d'identification (lieu et date de naissance etc.). Il commet cette faute au sein de l'État A, mais le préjudice subi par la victime est dans l'État B. Ce sera donc la loi de l'État B qui sera applicable. Cependant, le préjudice peut également être subi dans l'ensemble des États où l'image et/ou les informations personnelles de la victime ont été diffusées : le préjudice est alors multiple.

---

[189] CE, *Proposition de recommandations détaillées concernant le Règlement (CE) n°864/2007 sur la loi applicable aux obligations non contractuelles (Rome II) (2012).*
[190] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art.133 al.2.

Avantages et inconvénients

Le principal avantage de cette règle de conflits est le caractère juste et équitable à l'égard de la victime. D'autre part, le respect du principe de prévisibilité à l'égard de l'auteur du dommage est respecté.

Ce même avantage peut être relevé en matière de flux transfrontaliers de données à caractère personnel.

Toutefois, le principal inconvénient, à savoir le risque d'imprévisibilité est évité puisque les législations de chaque État exige le respect de la condition de prévisibilité.

En matière de flux transfrontaliers de données à caractère personnel, nous pouvons nous interroger sur les façons possibles de localiser l'atteinte au droit de la protection des données personnelles par le biais des flux transfrontaliers ? De la loi de l'État du traitement primaire ou secondaire, c'est-à-dire l'État de transmission ou l'État de réception des informations personnelles ? S'agit-il de l'État de résidence de la victime ?

Il semble que la localisation du préjudice doit se faire au sein de l'État de l'établissement de la « maison mère », ou bien de sa filiale.

C. Sur internet

Sur internet, la loi de l'État du préjudice revient à prendre en considération la loi de l'État de réception de l'information ou « *downloading* ».

Nous pouvons envisager ici l'interception d'une adresse courriel d'un individu par une tierce personne, et cela à des fins frauduleuses tels que l'envoi massif de « *spams* », pourriels ou courriers indésirables, ou encore l'envoi de courriels frauduleux ou « *phishing* ». En cas de litige, la loi applicable sera la loi de l'État où la victime a réceptionné le message envoyé.

Ainsi, dans l'affaire Guerbez c. Facebook,[191] les juridictions québécoises considèrent que l'application de la loi américaine comme loi de l'État de survenance du préjudice ne va pas à l'encontre de l'ordre public québécois, et cela malgré l'imprévisibilité à l'égard du

[191] *Facebook inc. c. Guerbez*, C.S.Q. Montréal, n. 500-17-053752-096, 28 septembre 2010, en ligne :
< http://fr.scribd.com/doc/38806669/Quebec-Superior-Court-judgment-against-Adam-Guerbuez#scribd > (consulté le 20 avril 2015).

défendeur à l'instance que cette solution présente. En l'espèce, une personne avait récupéré les adresses courriels des particuliers sur les réseaux sociaux ou autres sites à vocation publique, et avait par la suite envoyé une quantité infinie de pourriels, courriels indésirables.

La Cour supérieure du Québec constate que « *(...) La vente illégale de matériel pornographique, de drogue et de médicaments par une personne s'étant auparavant frauduleusement appropriée des données personnelles et s'étant fait passer pour quelqu'un d'autre afin de tromper ses propres clients ne peut que justifier en soi une telle condamnation. La solution la plus avantageuse malgré l'imprévisibilité qu'elle présente semble être le choix de la loi du lieu du préjudice* ».[192]

Avantages et inconvénients sur internet

Sur internet, les mêmes avantages que dans le cadre d'une situation prenant place hors internet peuvent être identifiés.

Le principal avantage demeure l'aspect équitable à l'égard de la victime. En effet, il parait assez juste pour le demandeur à l'instance que la loi applicable soit celle de l'État où l'information a été reçue. Dans bien des cas cette loi correspond à la loi du lieu de survenance du préjudice, et à certains égards, à la loi de l'État du domicile de la victime, mais pas toujours.

Cette solution doit être déterminée par chacun des systèmes juridiques étudié. En effet, l'article 15 alinéa 2 de la loi sur le Commerce électronique dispose que « *Au moment et lieu de l'expédition et de la réception d'un message de données* » dispose que : « *2. Sauf convention contraire entre l'expéditeur et le destinataire, le moment de la réception du message de données est défini comme suit : a) Si le destinataire a désigné un système d'information pour recevoir des messages de données : i) C'est le moment où le message de données entre dans le système d'information désigné; ii) Dans le cas où le message de données est envoyé à un autre système d'information du destinataire que le système désigné, c'est le moment où le message est relevé par le destinataire; b) Si le destinataire n'a pas désigné de système d'information,*

[192] *Facebook inc. c. Guerbez*, C.S.Q. Montréal, n. 500-17-053752-096, 28 septembre 2010, en ligne : < http://fr.scribd.com/doc/38806669/Quebec-Superior-Court-judgment-against-Adam-Guerbuez#scribd > (consulté le 20 avril 2015).

c'est le moment où le message de données entre dans un système d'information du destinataire ».[193]

Ainsi, d'après la disposition de la loi type de la CNUDCI,[194] il revient à chaque État de déterminer quelle disposition, parmi l'ensemble des dispositions précitées, sera mise en place aux fins d'apprécier la loi de la réception de l'information.

Les différentes possibilités de l'article 15 alinéa 2 de la loi sur le Commerce électronique[195] permettent d'éviter le risque de voir s'appliquer une multitude de lois.

Cependant, en l'absence de détermination par les États de la disposition applicable, ce critère peut présenter un caractère incertain.

D'autre part, dans le cas où le destinataire réceptionne le message alors qu'il se trouve en déplacement à l'étranger : la loi applicable sera la loi de l'État dans lequel le message litigieux est entré dans son système d'information ? Cela parait être effectivement le cas et nous amène à penser que ce critère peut entrainer une multiplicité des lois applicables et être imprévisible à l'encontre de l'auteur du dommage.

Concernant les flux transfrontaliers de données à caractère personnel, internet pourrait également avoir pour effet une multiplicité des lois applicables. Cependant, la combinaison de la loi de l'État de survenance du préjudice avec la loi de l'État de l'établissement de l'entreprise permettrait d'éviter cet inconvénient majeur.

Cette solution bien que profondément juste à l'égard de la victime et est prévisible à l'égard du défendeur à l'instance. Toutefois, ce critère ne semble pas encore tout à fait adapté à une situation prenant place sur internet et peut de ce fait présenter un caractère imprévisible à l'encontre de l'auteur du dommage.

---

[193] *Loi type de la CNUDCI sur le commerce électronique et guide pour son incorporation avec le nouvel article 5 bis tel qu'adopté en 1998,* Nations Unies, 1999, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 20 septembre 2015), art 15 al.2.
[194] *Id.*
[195] *Id.*

Section 2. La loi du lieu de la faute

A. Droit commun

En droit québécois, l'article 3126 du C.c.Q stipule que : « *L'obligation de réparer le préjudice causé à autrui est régie par la loi de l'État où le fait générateur du préjudice est survenu ».*[196]

En droit suisse, l'article 133 al.2 de la loi fédérale sur le droit international privé dispose que : « *Lorsque l'auteur et le lésé n'ont pas de résidence habituelle dans le même État, ces prétentions sont régies par le droit de l'État dans lequel l'acte illicite a été commis ».*[197]

Autrement dit, le droit international privé québécois et suisse prévoient que la loi applicable à un litige de nature extracontractuelle est la loi de l'État où la faute est survenue.

B. Application aux données personnelles

Une personne qui a commis une atteinte aux données personnelles dans un État A telle que la violation du droit à l'image d'un individu en la diffusant dans des journaux ou prospectus sans son consentement par exemple : ce sera la loi de l'État A, la loi où la diffusion de l'image, c'est-à-dire la loi où la faute a été commise, qui sera applicable.

Avantages et inconvénients

Le principal avantage de cette règle de conflits établissant comme solution la loi du lieu de la faute en matière de données personnelles, est le critère de prévisibilité à l'égard de l'auteur de l'acte préjudiciable. En effet, le défendeur à l'instance peut légitimement s'attendre à ce que la loi applicable soit celle où il a commis la faute. De plus, cette même loi peut dans bien des cas s'apparenter à la loi du lieu du domicile de l'auteur de l'acte dommageable.

---

[196] *Code civil du Québec,* L.Q., 1991, c. 64, art.3126.
[197] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 133 al.2.

Ce même avantage peut être relevé concernant les flux transfrontaliers de données à caractère personnel.

S'agissant des inconvénients, la loi du lieu de la faute peut paraitre profondément injuste, voir inéquitable à l'égard de la victime. En effet, il semble légitime de penser que l'auteur de l'acte peut choisir de commettre une faute dans un État où la législation se montre assez « indulgente » ou peu répréhensible en matière d'atteintes au droit de la protection des données personnelles. Dès lors, l'auteur peut prévoir d'y commettre une faute, en connaissance de cause, à savoir la faible probabilité que son acte soit sévèrement puni. Or pour la victime, une telle solution est injuste.

En matière de flux transfrontaliers de données à caractère personnel, l'entreprise pourrait commettre une faute en connaissance de cause, c'est-à-dire en sachant pertinemment que la loi applicable en cas de violation des données personnelles sera la loi du lieu de la faute, correspondant dans bien des cas au lieu du siège social ou de la filiale de l'entreprise, et ainsi choisir de s'établir dans un État où ce type d'atteintes n'est que très faiblement sanctionné.

Dès lors, il conviendrait de combiner ce critère de rattachement avec un ou d'autres critères afin d'éviter ce type de pratiques, et de ce fait léser la victime. Ainsi, la loi de l'État de survenance de la faute sur internet devrait être combinée par exemple avec la loi de l'État offrant « *la meilleure protection en matière de données à caractère personnel* »[198] que nous allons étudier. En d'autres termes, si la loi de la faute peut être définie comme celle offrant « *la meilleure protection en matière de données à caractère personnel »*[199] alors celle-ci sera prise en compte, et si ce n'est pas le cas, alors elle sera écartée.

C. Sur internet

Sur internet, la loi de l'État de survenance de la faute revient à prendre en considération la loi de l'État de transmission ou d'émission, « *uploading »* de l'information litigieuse.

---

[198] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[199] *Id.*

Nous pouvons imaginer le cas d'une personne X qui s'est procurée les informations (adresse courriel notamment) d'un individu Y de manière frauduleuse (récupération des adresses courriels par le biais des réseaux publics etc.). X se sert de cette adresse pour envoyer des « *spams* » ou pour récupérer d'autres informations personnelles, le cas de l'hameçonnage notamment. En cas de litige, la loi applicable, d'après ce facteur de rattachement, sera alors la loi de l'État de transmission ou d'émission de l'information. Ainsi, si X envoie son courriel frauduleux ou indésirable dans un État A alors que la victime est domiciliée dans un État B, ce sera la loi de l'État A qui sera applicable.

En droit français, le tribunal de grande instance de Paris a considéré dans une affaire Bénédicte S. c. Google inc. que : « *(…) le Règlement (CE) n.864/2007 du Parlement Européen et du Conseil du 11 juillet 2007, applicable aux obligations non contractuelles (« Rome II »), exclut de son champ d'application celles qui découlent d'atteintes à la vie privée et aux droits de la personnalité (…); Que l'application de la loi du pays où le dommage survient, au sens de l'article 4 de ce Règlement n'implique donc pas l'application de la loi française; Que la législation de l'État de Californie a en réalité vocation à s'appliquer, en raison de la production sur le territoire de l'État de Californie du fait générateur du dommage allégué, soit l'archivage des messages (…) ».*[200]

En d'autres termes, les juridictions françaises ont choisi comme critère de rattachement la loi de l'État où « *l'archivage des messages* »[201] sur internet a été produit, c'est-à-dire la loi californienne.

Avantages et inconvénients sur internet

Sur internet, les mêmes avantages qu'hors internet peuvent être soulevés.

En ce qui concerne les inconvénients, la loi de l'État de la faute parait davantage problématique. L'auteur d'un dommage peut avoir recours à un serveur localisé dans un État où la loi est plus clémente en matière d'atteintes au droit de la protection des données personnelles. Dès lors, l'auteur d'un tel acte n'a pas besoin de s'établir physiquement dans un

[200] TGI Paris, Ordonnance de référé (14 avril 2008).
[201] *Id.*

autre État afin d'éviter l'application de sanctions plus sévères en matière d'atteintes au droit de la protection des données personnelles. Cependant, à nouveau le recours à un serveur ne devrait jamais correspondre avec la loi du lieu de la faute.

Une question peut être soulevée : quels sont les critères permettant d'établir l'État dans lequel l'information litigieuse a été émise ou transmise sur internet ?

Afin d'éviter d'éventuelles fraudes de la part de l'auteur du dommage sur internet, le lieu de transmission de l'information litigieuse doit correspondre au lieu où l'auteur du dommage se trouvait « physiquement » au moment où il a porté atteinte au droit à la protection des données personnelles d'un individu. En d'autres termes, hors ou sur internet, la localisation de l'auteur du dommage est la même. Le recours aux nouvelles technologies afin d'éviter l'application de certaines lois ne doit pas être pris en considération.

En matière de flux transfrontaliers de données personnelles, les mêmes avantages sont susceptibles d'être relevés.

L'arrivée de l'Internet a accentué dans une certaine mesure les flux de données à caractère personnel. Toutefois, pour une entreprise l'application de la loi de l'État de la faute correspond bien souvent à la loi de l'État où l'entreprise, qui a traité de façon primaire et parfois secondaire l'information, est établie. De ce fait, il ne semble pas qu'internet favorise un contournement législatif de la part des entreprises, la seule loi prise en compte sera la loi de l'État où la faute a été commise, et bien souvent la loi d'établissement de l'entreprise ou celui de sa filiale.

La loi du lieu où la faute a été commise présente la particularité d'être prévisible à l'égard du défendeur. Toutefois, cette solution est injuste à l'égard de la victime.

L'utilisation d'internet n'a finalement pas pour effet d'aggraver ou d'accentuer cet inconvénient à l'égard de la victime.

Section 3. La loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance

A. Droit commun

En droit québécois, l'article 3126 alinéa 2 du C.c.Q dispose que : « *Dans tous les cas, si l'auteur et la victime ont leur domicile ou leur résidence dans le même État, c'est la loi de cet État qui s'applique ».*[202]

En droit européen, l'article 4 alinéa 2 du règlement Rome II applicable aux obligations non contractuelles stipule que : « *Toutefois, lorsque la personne dont la responsabilité est invoquée et la personne lésée ont leur résidence habituelle dans le même pays au moment de la survenance du dommage, la loi de ce pays s'applique ».*[203]

En droit suisse, l'article 133 al.1 de la loi fédérale sur le droit international privé dispose que : « *Lorsque l'auteur et le lésé ont leur résidence habituelle dans le même État, les prétentions fondées sur un acte illicite sont régies par le droit de cet État ».* [204]

Cette situation peut être susceptible de se produire dans plusieurs situations, à savoir notamment : une faute est survenue dans un État alors que les deux parties résident toutes les deux dans un autre État. Ainsi dans l'affaire Babcock c. Jackson,[205] plusieurs résidents des États-Unis décident de partir en voyage au Canada. En Ontario, Mr. Jackson, le conducteur, perd le contrôle de la voiture, et Mrs. Babcock est blessée. De retour aux États-Unis, Mrs Babcock décide de porter plainte contre le conducteur de la voiture. La question est alors de savoir quelle loi est applicable ? La loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance, c'est-à-dire la loi newyorkaise ou la loi de l'État de survenance de la faute, en l'occurrence la loi ontarienne. La Cour de New-York considère ici

---

[202] *Code civil du Québec,* L.Q., 1991, c. 64, art.3126.
[203] CE, *Règlement (CE) n. 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »),* 2007, en ligne :
< http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32007R0864&from=FR > (consulté le 7 mars 2015).
[204] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 133 al.1.
[205] *Babcock v. Jackson*, 191 N.E.2d 279 (N.Y. 1963).

que la loi ayant les liens les plus étroits avec le litige est la loi newyorkaise et non la loi ontarienne.

Cette situation peut également se produire dans le cas où la loi du lieu du préjudice subi par la victime est la loi du lieu où celle-ci est domiciliée, et la loi du lieu de la faute est également la loi du lieu du domicile du défendeur.

B. Application aux données personnelles

Il peut paraitre légitime de considérer que cette solution soit également applicable en matière d'atteintes au droit de la protection des données à caractère personnel.

Cette situation est effectivement susceptible de se produire : prenons l'exemple de l'auteur d'une atteinte aux données personnelles domicilié dans le même État que sa victime, l'État A. Cependant, il a commis l'acte litigieux dans un autre État, l'État B. En effet, le lieu de la faute peut être celui où l'auteur a son travail par exemple. La loi applicable sera alors la loi de l'État A.

Concernant les flux transfrontaliers de données à caractère personnel, la loi de l'État du domicile du défendeur correspond finalement à la loi de l'État où l'entreprise a son principal établissement.

Avantages et inconvénients

Le motif sous-jacent ici est le principe de proximité : nous n'appliquons ni la loi du lieu de la faute, ni celle du dommage pour plutôt appliquer la loi du « milieu commun » des parties, c'est-à-dire la loi ayant un lien plus étroit que la loi du lieu du délit ou la loi du lieu de la faute.

Dès lors, cette règle a la particularité d'être d'une part, relativement prévisible à l'égard de l'auteur du dommage, et d'autre part, de ne pas revêtir un caractère injuste, arbitraire voir inéquitable à l'égard de la victime.

Cette solution semble difficilement envisageable en pratique dans la mesure où l'application du droit international privé revêt par principe un élément d'extranéité puisqu'il doit s'agir dans la plupart des cas d'un conflit de lois nationales. Or, dans le cas où la loi du

lieu du domicile de la victime est souvent la loi du lieu où cette dernière a subi le préjudice, et d'autre part, que la loi du lieu de la faute est celle où l'auteur du dommage a son domicile, la situation en l'espèce ne présente aucun élément d'extranéité. Dès lors, cela conduit à l'écartement du droit international privé au profit du droit national. Toutefois, même s'il s'agit d'un cas exceptionnel, il est tout à fait possible de considérer que les deux parties peuvent résider au sein du même État mais le dommage ou la faute peuvent avoir été commis dans un État différent.

La situation ne change pas pour les flux transfrontaliers de données à caractère personnel.

C. Sur internet

La loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance ne semble pas revêtir de différence sur internet. Ce constat vaut également pour les atteintes au droit à la protection des données personnelles par le biais des flux transfrontaliers.

Ce critère est envisageable et intéressant dans la mesure où il s'agit d'une solution prévisible à l'égard de l'auteur, ainsi que juste et équitable pour la victime d'une atteinte aux données personnelles.

Section 4. La loi de l'État de la résidence habituelle du défendeur à l'instance

A. Droit commun

En droit européen, l'article 5 bis alinéa 2 de la proposition de modification du Règlement Rome II dispose que : « *Toutefois, la loi applicable est la loi du pays dans lequel le*

défendeur a sa résidence habituelle si celui-ci ne pouvait pas avoir raisonnablement prévu les conséquences importantes de son acte dans le pays désigné par le paragraphe 1 ».[206]

Autrement dit lorsqu'il n'est pas possible d'appliquer la loi du lieu du préjudice en raison de son caractère imprévisible, on appliquera la loi du lieu de résidence principale du défendeur à l'instance.

B. Application aux données personnelles

Nous pouvons envisager le cas d'un individu X résidant dans un État A qui diffuse des images, ou le lieu et la date de naissance et l'adresse postale d'une personne Y et domiciliée dans un État B par le biais de prospectus par exemple. Au regard de cette solution, la loi applicable en cas de litige, sera la loi de l'État A où l'individu Y auteur du dommage réside.

En matière de flux transfrontaliers de données à caractère personnel, la loi de l'État de résidence du défendeur à l'instance correspond à la loi de l'État de l'établissement principal de l'entreprise.

Avantages et inconvénients

Le principal avantage semble être le fait que, et cela contrairement au choix du lieu de survenance de la faute, l'auteur ne puisse pas choisir la loi de l'État où les atteintes relatives aux données personnelles sont peu sanctionnées. En effet, il parait difficile pour l'auteur d'un tel acte de modifier le lieu de son principal établissement, c'est-à-dire de « déménager » afin de pouvoir commettre une faute au sein d'un État où les sanctions inhérentes à ce type d'actes ne sont que très peu répressives. Dès lors, la loi du lieu du principal établissement de l'auteur de l'acte semble être moins « flexible » et/ou souple que la loi du lieu de la faute.

D'autre part, cette solution est prévisible à l'égard de l'auteur de l'acte. En effet, il n'y a pas plusieurs lois applicables mais seulement une loi, celle de la loi du lieu où le défendeur à l'instance a son principal établissement.

---

[206] PARLEMENT EUROPÉEN, *Rapport contenant des recommandations à la Commission sur la modification du règlement (CE) n°864/2007 sur la loi applicable aux obligations non contractuelles (Rome II),* Bruxelles, 2 mai 2012, en ligne : < http://www.alain-bensoussan.com/wp-content/uploads/22798084.pdf > (consulté le 14 mars 2015).

Ce critère de rattachement peut paraitre profondément injuste, inéquitable et arbitraire au regard de la victime.

À cet égard, il est possible d'imaginer qu'une personne porte atteinte aux données personnelles d'un individu en sachant pertinemment qu'au sein d'un État dans lequel il a sa résidence principale, les atteintes relatives aux données personnelles ne sont que très peu sanctionnées. Or cela aura pour conséquence de léser la victime.

En ce qui concerne les flux transfrontaliers des données à caractère personnel, le choix de la loi de l'État de résidence du défendeur à l'instance s'apparentant à la loi de l'État où l'entreprise a son principal établissement présente les mêmes avantages et inconvénients. Encore une fois, une entreprise peut choisir intentionnellement de s'établir dans un État où la législation en matière de protection des données personnelles est particulièrement souple, ce qui peut avoir pour effet de léser la victime.

C. Sur internet

Sur internet, les atteintes aux données personnelles sont par nature plus facilement accessibles à un plus grand nombre d'utilisateurs dans différents États pouvant conduire à une multiplication du préjudice : ce critère de rattachement permet donc d'éviter une multiplicité des lois applicables.

Les mêmes inconvénients hors et sur internet peuvent être identifiés.

Sur internet, la situation ne change pas pour les atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers.

Cette solution parait envisageable dans la mesure où elle apparait finalement comme une alternative à la loi du lieu de survenance du préjudice, loi susceptible de revêtir un caractère imprévisible. Toutefois, dans le cas où l'auteur a commis une atteinte aux données personnelles dans son État de résidence en sachant pertinemment que la la loi de cet État ne sanctionne que très faiblement ce type d'atteintes, ce critère de rattachement peut alors paraitre injuste à l'égard de la victime.

Cependant, cette solution ne doit pas pour autant être écartée.

Section 5. La loi de l'État favorisant la victime

Il s'agit ici d'une disposition particulière prévue par le droit suisse en matière d'atteintes aux droit de la personnalité (A.). Ce critère de rattachement sera ensuite appliqué aux données personnelles (B.), puis sur internet (C.).

A. Disposition particulière

L'article 139 alinéa 1 de la loi fédérale sur le droit international privé suisse laisse le choix à la victime d'une atteinte aux droits de la personnalité de choisir entre plusieurs lois : « *Les prétentions fondées sur une atteinte à la personnalité par les médias, notamment par la voie de presse, de la radio, de la télévision ou tout autre moyen public d'information, sont régies, au choix du lésé :*

a. *Par le droit de l'État dans lequel le lésé a sa résidence habituelle, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État ;*
b. *Par le droit de l'État dans lequel l'auteur de l'atteinte à son établissement ou sa résidence habituelle, ou*
c. *Par le droit de l'État dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État ».*[207]

Autrement dit, cette solution donne la possibilité à la victime de choisir entre plusieurs lois, et donc de choisir la loi qui lui sera le plus favorable.

B. Application aux données personnelles

L'alinéa 3 de l'article 139 de la loi sur le droit international privé suisse dispose que : « *l'al. 1 s'applique également aux atteintes à la personnalité résultant du traitement de*

[207] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 139 al.1.

données personnelles ainsi qu'aux entraves mises à l'exercice du droit d'accès aux données personnelles ».[208]

En d'autres termes, la victime d'une atteinte aux données personnelles pourra choisir la loi de l'État où elle a sa résidence habituelle avec une condition de prévisibilité pour l'auteur du dommage, ou la loi de l'État dans lequel l'auteur a sa résidence habituelle ou enfin la loi de l'État de survenance du dommage avec encore une fois la condition de prévisibilité à l'égard de l'auteur.

En matière de flux transfrontaliers, la loi de l'État du domicile du défendeur revient à prendre en considération la loi de l'État où l'entreprise a son principal établissement.

Avantages et inconvénients

Bien évidemment cette solution est très avantageuse et profondément juste à l'égard de la victime. Elle pourra alors choisir la loi qui lui semble être la plus favorable.

Cette solution peut paraitre injuste à l'encontre du défendeur dans la mesure où l'imprévisibilité demeure. En effet, l'auteur ne peut pas prévoir quelle loi sera applicable dans la mesure où plusieurs lois (une loi parmi trois) seront susceptibles d'être appliquées.

Cependant, la condition de prévisibilité est énoncée dans le cadre de l'alinéa a) et c) : la loi applicable pourra être la loi de l'État du domicile de la victime ou la loi de l'État de survenance du dommage.

Concernant les flux transfrontaliers de données à caractère personnel, la situation ne semble pas revêtir de particularités.

C. Sur internet

Sur internet, la situation ne change pas. Au contraire, ce choix laissé à la victime témoigne de la parfaite adaptabilité du droit suisse à des situations prenant place sur internet.

---

[208] *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291, art. 139 al.3.

Ce constat est le même s'agissant des flux transfrontaliers de données à caractère personnel.

Cette solution est donc tout à fait envisageable car elle est juste et avantageuse à l'égard de la victime, et respecte le principe de prévisibilité envers l'auteur du dommage.

À présent, les facteurs de rattachement étudiés ne relèvent plus du droit commun, mais de la doctrine : certains sont reconnus par la doctrine, d'autres non. Les critères suivants, à savoir l'accessibilité (section 6), le ciblage (section 7), la loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires (section 8) ont été envisagés par la doctrine pour des situations prenant place uniquement sur internet.

Les facteurs de rattachement ne seront pas une nouvelle fois présentés de manière générale dans la mesure où cela a déjà été fait ci-dessus (Chapitre 1 : Données personnelles et compétence internationale des tribunaux québécois, européen et suisse) mais directement appliqués aux données personnelles. L'étude de ces facteurs dans le cadre d'une situation prenant place sur internet n'est ici pas nécessaire.

Section 6. L'accessibilité

A. Présentation générale

L'accessibilité a déjà été présentée dans le chapitre 1. Il n'est donc pas nécessaire de présenter ce critère une nouvelle fois.

B. Application aux données personnelles

Si nous prenons l'exemple d'une violation du droit à l'image d'une personne, cette image sera accessible par un grand nombre d'internautes et dans beaucoup de pays. De la même manière, l'inscription sur un site internet du numéro d'assurance sociale, du sexe, de l'âge, du numéro de téléphone ou encore de l'adresse courriel d'un individu par une tierce personne, l'ensemble de ces informations sera accessible par un nombre important d'individus et dans le monde entier.

Cette solution ne semble pas correspondre à un cas d'atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers. Nous pouvons alors imaginer le cas où des entreprises « revendent » des informations personnelles à d'autres entreprises. Ces dernières exploitent et rendent accessibles, les informations achetées sur des sites internet. Cette situation parait peu probable dans la mesure où les sociétés seraient identifiées sur la toile et ensuite très certainement sanctionnées pour fraudes.

Avantages et inconvénients

Ce facteur de rattachement peut s'apparenter à certains égards à la loi de l'État où le préjudice est subi ou encore à la loi de l'État de la résidence principale de la victime.

Dès lors, cette solution présente un caractère juste et équitable à l'égard de la victime.

Toutefois, cette solution peut revêtir un aspect imprévisible à l'encontre du défendeur à l'instance. D'autre part, si la simple accessibilité d'un site suffit à l'application d'une loi, il est dès lors plausible de penser qu'une pluralité de lois soit ici applicable pour un même litige.

Ce critère n'a donc pas d'existence autonome.

L'accessibilité est un facteur intéressant lorsqu'il permet de conforter le choix de telle ou telle loi notamment la loi du lieu de survenance du préjudice. Cependant, cette solution ne doit en aucun cas être prise de manière autonome en raison du caractère imprévisible qu'elle est susceptible de revêtir à l'égard de l'auteur du dommage.

Section 7. Le ciblage

A. Présentation générale

La jurisprudence québécoise « *n'a pas directement traité du critère du ciblage* ».[209] À cet égard, il convient de rappeler que les juridictions appliquent « *les règles de conflits normales* ».[210]

---

[209] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*
[210] *Id.*

Monsieur le Professeur Gérald Goldstein met en avant le fait que : « *la prévisibilité est la condition nécessaire à l'application de la loi du lieu du préjudice, dans l'article 3126 du C.c.Q., cette exigence pourrait certainement se caractériser par la preuve d'un ciblage de la part de l'auteur de la faute. Toutefois aucun arrêt n'a jusqu'à présent directement fondé son raisonnement sur cette notion ».*[211]

Autrement dit, la preuve qu'une personne a intentionnellement ciblé cet État et non un autre doit être établie : l'auteur du dommage pourra alors raisonnablement prévoir que la loi de l'État ciblé soit applicable.

Monsieur le Professeur Gérald Goldstein poursuit son analyse en considérant que le ciblage pourrait être considéré comme un élément à prendre en compte, et cela parmi d'autres, afin d'appliquer la clause échappatoire prévue par l'article 3082 du C.c.Q. qui dispose que: « *À titre exceptionnel, la loi désignée par le présent livre n'est pas applicable si, compte tenu de l'ensemble des circonstances, il est manifeste que la situation n'a qu'un lien éloigné avec cette loi et qu'elle se trouve en relation beaucoup plus étroite avec la loi d'un autre État. La présente disposition n'est pas applicable lorsque la loi est désignée dans un acte juridique ».*[212]

La jurisprudence française l'envisage comme un critère de rattachement lorsqu'il est combiné avec d'autres facteurs de rattachement, à savoir le lieu de la faute notamment.

B. Application aux données personnelles

En droit français, le tribunal de grande instance de Paris a considéré dans l'arrêt Bénédicte s c. Google inc., que: « *Que la législation de l'État de Californie a en réalité vocation à s'appliquer, en raison de la production sur le territoire du fait générateur du dommage allégué, soit l'archivage des message; que les plus anciens d'entre eux qui révèlent plus particulièrement des sujets d'intérêt touchant à la vie personnelle de la demanderesse*

[211] GOLDSTEIN, G., « Droit international privé et immatériel (Rapport québécois) », *Henri Capitant.*
[212] *Code civil du Québec,* L.Q., 1991, c. 64, art. 3082.

sont au surplus diffusés par l'auteur en langue anglaise, principalement à destination d'internautes résidant aux États-Unis d'Amérique ».[213]

En d'autres termes, il semble que la juridiction française se réfère au ciblage pour conforter l'application de la loi de l'État où la faute a été commise mais ne l'envisage pas en tant que critère autonome. À cet égard, le fait que les messages « *touchant à la vie personnelle de la demanderesse sont au surplus diffusés par l'auteur en langue anglais, principalement à destination d'internautes résidant aux États-Unis d'Amérique »*[214] vient finalement « compléter » la prise en compte de la loi du lieu de la faute.

Cette solution ne semble pas réellement applicable en cas d'atteintes au droit de la protection des données personnelles par le biais des flux transfrontaliers.

Avantages et inconvénients

Ce critère a la particularité d'être prévisible à l'égard du défendeur à l'instance. En effet, il parait possible de considérer que cette solution entraine une prévisibilité dans la mesure où l'auteur du dommage peut s'attendre à ce que la loi appliquée soit celle de l'État initialement ciblé.

D'autre part, ce facteur de rattachement peut paraitre juste et équitable à l'égard de la victime dans la mesure où l'État ciblé sera celui où la victime a subi le préjudice et dans bien des cas, l'État du lieu où cette dernière a son domicile principal.

Cependant, le caractère extrêmement prévisible de ce facteur de rattachement peut paraitre injuste voir inéquitable à l'égard de la victime dans la mesure où l'auteur d'un dommage peut choisir de cibler spécifiquement tel ou tel État eu égard au fait que la loi de ce dernier est particulièrement clémente en matière d'atteintes aux données personnelles.

Dès lors, pour éluder cet inconvénient il conviendrait de prendre en compte la loi où la victime a subi le dommage est le plus considérable avec la prise en compte de l'intention par l'auteur de « cibler » cet État spécifiquement. Cette loi aurait alors vocation à connaitre de l'ensemble

---

[213] TGI Paris, Ordonnance de référé (14 avril 2008).
[214] *Id.*

des dommages subi dans les autres États par la victime. Finalement, cela reviendrait en droit québécois à appliquer, avec la condition de prévisibilité. L'article 3126 alinéa 1 du Code civil du Québec qui prévoit que : « *L'obligation de réparer le préjudice causé à autrui est régie par la loi de l'État où le fait générateur du préjudice est survenu. Toutefois, si le préjudice est apparu dans un autre État, la loi de cet État s'applique si l'auteur devait prévoir que le préjudice s'y manifesterait ».*[215]

Cette solution est intéressante mais n'a pas d'existence autonome dans la mesure où elle doit être associée à un autre facteur de rattachement. En effet, le ciblage, de la même manière que l'accessibilité, ne peut être utilisé que pour conforter le choix de la loi du lieu du préjudice par exemple, ou du lieu de la faute. Il n'est pas possible d'avoir recours à ce facteur de manière autonome dans la mesure où pris de façon individuel, il est susceptible de présenter un caractère injuste et arbitraire à l'égard de la victime.

Section 8. La loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires

A. Présentation générale

Ce critère ayant également déjà été présenté dans le chapitre 1, il s'agit directement d'appliquer la loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires aux données personnelles.

B. Application aux données personnelles

En matière d'atteintes au droit de la protection des données personnelles, nous pouvons envisager la diffusion d'une image ou d'un élément permettant l'identification d'une personne (nom, prénom etc.) sur un site internet par une tierce personne, et cela sans le consentement du principal intéressé. La loi applicable d'après cette solution, sera alors la loi de l'État où le fournisseur d'accès à internet, ou de l'hébergeur de l'information ou encore de l'intermédiaire

[215] *Code civil du Québec,* L.Q., 1991, c. 64, art.3126.

est établi. Ainsi dans le cas où la victime d'une atteinte à ses données personnelles est domiciliée dans un État A, que l'auteur du dommage est établi dans un État B, et que le fournisseur d'accès à internet, ou l'hébergeur ou encore l'intermédiaire est établi dans un État C, la loi applicable sera alors la loi de l'État C.

Avantages et inconvénients

Le principal avantage demeure une nouvelle fois l'aspect prévisible de ce facteur de rattachement à l'égard de l'auteur du dommage : seul sera applicable la loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires.

Cependant, cette solution revêt un aspect arbitraire et injuste à l'égard de la victime. En effet, il parait possible de penser que le défendeur à l'instance utilise un fournisseur d'accès à internet ou un hébergeur situé dans un État où la législation ne sanctionne que très faiblement les atteintes au droit à la protection des données personnelles.

D'autre part, une problématique demeure : quels sont les critères permettant d'établir la loi de l'État du fournisseur d'accès à internet ou de l'hébergeur ou des intermédiaires ? Quelle loi sera applicable lorsque l'État du fournisseur etc. est anonyme (exemple avec le réseau *Tor*) ? Encore une fois, il semble que ce facteur de rattachement n'est pas d'existence autonome et doit de ce fait être combiné avec les règles de conflits traditionnelles.

La situation ne change pas en ce qui concerne les atteintes au droit à la protection des données personnelles par le biais des flux transfrontaliers.

Ce critère de rattachement, en raison de son absence de proximité avec le litige et du caractère arbitraire et injuste que cela fait peser sur les victimes ne semble pas envisageable.

Les deux critères de rattachement suivants, à savoir la loi de l'État « *offrant la meilleure protection des données à caractère personnel* »[216] (section 9), et la loi de l'État où est établi le « *maître du fichier* » [217] (section 10) ont été imaginés pour des situations

[216] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[217] *Id.*

concernant directement des atteintes au droit de la protection des données personnelles par le biais de flux transfrontaliers hors et également sur internet.

Pour chacun des facteurs de rattachement, une présentation générale (A) et la situation sur internet seront successivement présentées (B).

Section 9. La loi de l'État « *offrant la meilleure protection des données à caractère personnel* »[218]

A. Présentation générale

Ce critère de rattachement a notamment été envisagé par Monsieur le Professeur Karim Benyekhel en matière de flux transfrontaliers de données à caractère personnel. Il s'agit finalement de prendre en compte la loi de l'État qui offrira à la victime la meilleure protection de ses données, c'est-à-dire la loi porposant les meilleures garanties afin de protéger les données personnelles d'un individu. Il semble que pour être applicable, cette loi doit avoir un lien avec le litige.

Nous pouvons imaginer le cas d'une entreprise établie aux Etats-Unis qui porte atteinte aux données personnelles d'un individu. La victime décide alors de porter plainte devant le tribunal de l'État de son domicile situé au sein d'un État membre de l'Union européenne par exemple. Le tribunal de l'État saisi peut alors choisir d'appliquer, non pas la loi de l'État où l'entreprise est établie, en l'occurrence la loi américaine, mais la loi « *offrant la meilleure protection des données à caractère personnel* »,[219] et cela parmis les lois ayant un lien avec le litige : la loi de l'État du domicile de la victime ou encore la loi de l'État de survenance du préjudice. À cet égard, la législation européennne étant plus protectrice en matière de données personnelles, il serait fort probable de penser que la loi applicable soit alors la loi d'un des États membres de l'Union européenne.

---

[218] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[219] *Id.*

En ce qui concerne la loi de l'État de survenance du préjudice, l'entreprise peut avoir transférer les informations personnelles d'un individu dans un nombre important d'États. Dès lors, le préjudice peut être constitué au sein de l'ensemble de ces États. En effet, l'entreprise peut choisir de transférer des informations à d'autres entreprises à des fins commerciales. Les fichiers avec les numéros de téléphone, les adresses courriels ou toutes autres informations susceptibles d'identifier un individu peuvent être communiqués. La personne recevra alors des courriels ou des appels téléphoniques commerciaux, qui peuvent également être frauduleux (dans le but d'extorquer des fonds à la personne) : le préjudice sera alors subi au domicile de cette personne. Or, si l'on reprend l'exemple mentionné ci-dessus, l'individu domicilié au sein d'un État membre de l'Union européenne bénéficiera de la législation européennne relative à la protection des données personnelles, législation relativement protectrice en la matière.

À première vue, cette solution semble s'apparenter à la loi de l'État favorisant la victime prévu par le droit suisse notamment.

Avantages et inconvénients

Ce critère de rattachement présente l'avantage d'être particulièrement juste à l'égard de la victime puisque la loi applicable sera celle qui protège le mieux ses données personnelles.

Cependant, cette solution est empreinte d'incertitudes dans la mesure où il faudra attendre l'issue du procès pour connaitre la loi applicable. À cet égard, l'OCDE a considéré que : « *En revanche, on peut faire valoir que des solutions de ce type laissent planer trop d'incertitude, en particulier du point de vue des maîtres de fichier qui pourront souhaiter connaitre, s'il y a lieu à l'avance, à quel ensemble de règles nationales un système international de l'information sera soumis ».*[220]

Contrairement à la solution prévue en droit suisse, ce critère de rattachement n'énonce pas les différentes lois susceptibles de favoriser la victime, et ne prévoit aucunement le respect de la condition de prévisibilité à l'égard du défendeur à l'instance.

---

[220] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.

B. Sur internet

Sur internet, la situation ne change pas véritablement. En effet, l'utilisation d'internet ne permet pas de favoriser l'application d'une multitude de lois puisqu'ici il s'agit avant tout de prendre en compte la loi « *offrant la meilleure protection des données à caractère personnel* ».[221]

Cette solution est intéressante dans la mesure où elle très protectrice envers la victime d'une atteinte à ses données personnelles par le biais des flux transfrontaliers. Toutefois, ce critère n'est pas envisageable en raison de son caractère imprévisible. À cet égard, l'imprévisibilité inhérente à ce critère de rattachement permet de le distinguer d'un autre critère étudié ci-dessus, à savoir la loi favorisant la victime prévue notamment par le droit suisse. En effet, cette solution met en avant le choix pour la victime entre plusieurs facteurs de rattachement, et prévoit que pour être applicable la solution choisie doit être prévisible à l'égard du défendeur.

Section 10. La loi de l'État où est établi le « *maître du fichier* »[222]

A. Présentation générale

Ce facteur de rattachement, prévu pour les flux transfrontaliers de données à caractère personnel, a également été mis en avant par le Professeur de l'Université de Montréal, Karim Benyekhel.

Le « *maître de fichier* »[223] est la personne physique ou morale qui est déclaré responsable du fichier contenant les informations personnelles d'un individu. De ce fait, la loi correspondant à l'État où est établi le « maître du fichier » pourrait s'apparenter à la loi de l'État où l'entreprise est établie, mais pas nécessairement. En effet, nous pouvons imaginer le cas d'une entreprise établie au sein d'un État européen et ayant un responsable des fichiers au sein d'un autre État par exemple.

---

[221] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[222] *Id.*
[223] *Id.*

Avantages et inconvénients

Ce critère de rattachement présente la particularité d'être prévisible à l'égard de l'auteur du dommage dans la mesure où la seule loi applicable sera celle de l'État où est établi le « *maître du fichier* ».[224]

Le principal inconvénient semble être la difficulté d'identification du « *maître du fichier* ».[225] Or cette contrainte peut favoriser les cas de la multiplicité des lois applicables, et également les cas de fraude à la loi dans la mesure où l'auteur peut choisir un État où la législation en matière d'atteintes au droit de la protection des données personnelles est particulièrement faible.

Comment est-il possible de localiser le « *maître du fichier »*[226] S'agit-il de l'entreprise ayant traité de façon primaire ledit fichier ? Où secondaire ? De l'entreprise ayant stocké l'information ? [227]

La localisation de la personne morale ou physique responsable d'un fichier contenant des informations personnelles devrait être l'entreprise ayant traité de façon primaire l'information, et non s'il y a lieu, le sous-traitant.

De manière générale, cette loi devrait être considérée comme n'ayant pas de liens étroits avec la situation.

B. Sur internet

Sur internet, la situation ne change pas : les cas de fraude à la loi ou les cas de multiplication de lois ne semblent pas être favorisés.

Cette solution n'a finalement aucun lien étroit avec la situation, et n'est dès lors pas envisageable en cas de litige.

---

[224] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[225] *Id.*
[226] *Id.*
[227] *Id.*
.

Synthèse

Certaines solutions sont tout à fait envisageables et d'autres absolument pas. Parmi les solutions envisageables, certaines présentent principalement que des avantages et d'autres bien qu'envisageables, présentent des inconvénients. D'autre part, certaines solutions n'ont pas d'existence autonome mais pourraient être envisagées avec d'autres facteurs de rattachement.

Parmi les solutions qui semblent tout à fait envisageables, il y a la loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance ainsi que la loi favorisant la victime.

La loi de l'État du domicile ou de résidence principale du demandeur et du défendeur à l'instance prévue notamment par le droit québécois, le droit européen et le droit suisse est une solution qui présente l'avantage d'être prévisible à l'égard de l'auteur et particulièrement juste et équitable pour la victime.

De la même manière, la loi favorisant la victime envisagée par le droit suisse est une solution juste et avantageuse à l'égard de la victime et la condition de prévisibilité est respectée à l'égard de l'auteur.

D'autres solutions sont envisageables mais présentent certains inconvénients, à savoir : la loi du lieu de survenance du préjudice, la loi du lieu de la faute ou encore la loi de l'État de résidence du défendeur à l'instance.

La loi du lieu du préjudice, prévue par le droit québécois, par la proposition de modification du Règlement européen Rome II et par le droit suisse, est envisageable dans la mesure où elle est profondément juste à l'égard de la victime.

Cependant, cette solution peut revêtir un caractère imprévisible à l'encontre de l'auteur du dommage et cela peut être accentué avec l'utilisation d'internet.

En effet, sur internet, la loi du lieu du préjudice correspond à la loi du lieu de réception de l'information, « *downloading* ». La loi type de la CNUDCI[228] prévoit que chaque État doit

[228] *Loi type de la CNUDCI sur le commerce électronique et guide pour son incorporation avec le nouvel article 5 bis tel qu'adopté en 1998,* Nations Unies, 1999, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 20 septembre 2015).

choisir quelle disposition, parmi l'ensemble proposé par l'article 15 al.2,[229] il souhaite mettre en place afin d'apprécier la loi de réception de l'information. Or en l'absence de détermination par les États de la disposition applicable, ce critère devient incertain.

La loi du lieu de la faute envisagée en droit québécois et en droit suisse est prévisible à l'égard du défendeur mais injuste à l'égard de la victime. D'autre part, internet n'a pas pour effet d'aggraver ou d'accentuer cet inconvénient à l'égard de la victime.

Sur internet, la loi du lieu de la faute est la loi de l'émission ou de la transmission de l'information, « *uploading* ».

La loi de l'État de résidence du défendeur à l'instance envisagée notamment par le droit européen apparait finalement comme une alternative à la loi du lieu de survenance du préjudice, loi susceptible de revêtir un caractère imprévisible. Toutefois, dans le cas où l'auteur a commis une atteinte aux données personnelles dans son État de résidence en sachant pertinemment que la loi de cet État ne sanctionne que très faiblement ce type d'atteintes, ce critère peut alors paraitre injuste à l'égard de la victime.

Certaines solutions, envisagées par la doctrine, sont intéressantes dans la mesure où elles permettent de « conforter » le choix de telle ou telle loi mais n'ont pas d'existence autonome, notamment l'accessibilité et le ciblage dans le cadre d'une situation prenant place sur internet.

Le critère de l'accessibilité ne peut être pris de manière autonome en raison du caractère imprévisible qu'il est susceptible de revêtir à l'égard de l'auteur du dommage.

Le ciblage peut présenter un caractère injuste et arbitraire à l'égard de la victime lorsqu'il est pris de manière autonome.

Enfin, certaines solutions prévues par la doctrine dans le cadre de situations prenant place sur internet ne sont tout simplement pas envisageables.

---

[229] *Loi type de la CNUDCI sur le commerce électronique et guide pour son incorporation avec le nouvel article 5 bis tel qu'adopté en 1998,* Nations Unies, 1999, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 20 septembre 2015), art 15 al.2.

La loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires ne peut être envisageable en raison de son absence de proximité avec le litige et du caractère arbitraire et injuste que cela fait peser sur la victime.

La loi de l'État « *offrant la meilleure protection des données à caractère personnel* »[230] est très protectrice envers la victime mais trop imprévisible à l'égard de l'auteur du dommage.

La loi de l'État où est établi le « *maître du fichier* »[231] ne présente aucun lien étroit avec la situation et n'est dès lors pas envisageable.

Enfin s'agissant des lois de police, le juge saisi du litige pourrait choisir d'appliquer sa propre loi aux fins de ne pas léser la victime d'une atteinte au droit de la protection des données personnelles. À cet égard, lorsqu'il s'agit du contenu des données personnelles, il est possible de penser que le litige dépend de la loi personnelle, et concernant la violation de l'obligation légale de ne pas porter préjudice à autrui alors cela dépend du quasi-délictuel. Dans les deux cas, la notion de lois de police est une solution très attractive dans la mesure où ce qui concerne la personne relève de l'ordre public, et les quasi-délits, en raison de leur nature proche du droit pénal, ont favorisé leur proximité théorique avec les lois de police ou d'ordre public.

À noter qu'en droit français, le nom relève du statut personnel et donc de la loi personnelle : dès lors toute diffusion du nom d'une personne sans son consentement par une tierce personne entrainera l'application de la loi française si la victime est française.

---

[230] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[231] *Id.*

Conclusion

Cette étude s'est révélée particulièrement intéressante et enrichissante. Il était important de bien délimiter les termes du sujet et de ne traiter que des données personnelles et non de la vie privée et de la diffamation.

La définition de « données personnelles » avec les éléments devant y être inclus ou exclus, s'est avérée dans un premier temps assez difficile dans la mesure où cette notion est parfois ambivalente, et peut être rapprochée du terme de « vie privée ».

Un schéma est donc apparu nécessaire pour clarifier les éléments devant être inclus dans le sujet, et ceux pouvant y être exclus car ne relevant pas du domaine de la protection des données personnelles.

L'application des données personnelles au droit international privé s'avère aujourd'hui nécessaire dans la mesure où les situations étudiées s'avèrent de plus en plus susceptibles de se produire notamment avec l'arrivée de l'Internet au sein des foyers.

Hors et sur internet, la situation change finalement assez peu. Certains inconvénients peuvent être aggravés notamment en ce qui concerne le tribunal de l'État de survenance du préjudice ou de la loi applicable au préjudice puisque le dommage est alors susceptible de survenir dans plusieurs États, voir le monde entier, ce qui a pour effet de multiplier les fors compétents mais également les lois applicables. Toutefois, la condition de prévisibilité exigée par les législations québécoise, européenne et suisse en matière de conflits de lois permettent d'éviter cette situation.

À cet égard, sur internet la doctrine a envisagé certains facteurs de rattachement, facteurs ne relevant pas du droit commun. Certains de ces critères se sont révélés être intéressants et pourraient être envisageables selon certaines conditions, et d'autres absolument inenvisageables.

L'analyse du sujet a conduit à « extraire » les solutions les plus favorables au regard des principes inhérents au droit international privé, à savoir notamment : la bonne administration de la justice, l'équité procédurale, la prévisibilité à l'égard du défendeur à

l'instance, l'existence de liens suffisants entre le tribunal saisi et le litige en cause, la détermination du centre des intérêts et le principe de proximité.

En matière de compétence juridictionnelle, plusieurs solutions prévues notamment en droit commun, se sont avérées intéressantes : le tribunal de l'État de survenance du préjudice, le tribunal de l'État de survenance de la faute, le tribunal de l'État du domicile du défendeur et le tribunal de l'État du domicile de la victime.

Le tribunal de l'État de survenance du préjudice est une solution juste et équitable à l'égard de la victime mais elle peut être imprévisible à l'encontre de l'auteur du dommage.

Le tribunal de l'État de survenance de la faute est prévisible envers le défendeur à l'instance mais injuste à l'égard de la victime puisque l'auteur peut choisir de commettre une atteinte au droit de la protection des données personnelles en fonction de la loi que le tribunal de l'État saisi appliquera.

Le tribunal de l'État du domicile du défendeur est une solution prévisible envers l'auteur du dommage mais injuste et inéquitable à l'égard de la victime qui sera alors contraint de se déplacer au sein d'un autre État. De plus, on ne peut pas exclure la possibilité que l'auteur du dommage ait choisi de commettre une atteinte au droit à la protection des données personnelles au sein de l'État de son domicile en fonction de la loi que ce tribunal appliquera une fois saisi, loi pouvant être particulièrement clément en matière d'atteintes aux données personnelles par exemple.

Enfin le tribunal de l'État du domicile de la victime est une solution intéressante puisqu'elle est finalement assez prévisible pour le défendeur à l'instance, et en même temps juste et équitable, voir même favorable à la victime. Cependant, elle peut paraitre injuste à l'encontre de l'auteur si ce dernier a vocation à se déplacer devant les tribunaux d'un État différent que celui de son domicile.

Pour éviter une multiplicité des fors compétents notamment sur internet, le tribunal de l'État du domicile de la victime ou le tribunal de l'État du domicile de l'auteur du dommage semblent être des choix plus judicieux.

D'autres solutions, peuvent être mentionnées dans la mesure où il s'agit de solutions intéressantes mais ne sont pas réellement envisageables : l'accessibilité, le ciblage, et le tribunal du centre principal des intérêts du demandeur.

L'accessibilité, le ciblage et le tribunal du centre principal des intérêts du demandeur n'ont été envisagées par la doctrine ou par la Cour de Justice de l'Union européenne que dans le cadre de situations prenant place sur internet, ce qui n'est pas le cas avec le tribunal de l'État avec lequel la cause présente un lien suffisant.

L'accessibilité est une solution intéressante mais n'a pas d'existence autonome puisque ce n'est pas le critère en tant que tel qui va donner compétence aux tribunaux d'un État mais finalement le lieu de la faute ou du dommage. Ce facteur de rattachement conforte, appuie le choix de tel tribunal au lieu d'un autre. Pris de manière à part entière, ce facteur de rattachement aura pour effet une multiplicité des fors compétents dans la mesure où l'information litigieuse sera accessible dans le monde entier.

Le ciblage est une solution prévisible à l'égard du défendeur. Toutefois, en matière de protection des données personnelles, les éléments permettant d'établir la volonté de l'auteur du dommage de cibler un État en particulier peuvent s'avérer difficiles à identifier. Or il est nécessaire de l'établir afin d'éviter la possibilité qu'une multitude de tribunaux se déclarent compétents. Ce critère pourrait néanmoins permettre d'appuyer, de conforter la compétence du tribunal de l'État de la faute ou du tribunal du préjudice par exemple.

Le tribunal du centre principal des intérêts du demandeur est une solution juste et équitable à l'égard de la victime et permet également d'éviter une multiplication des fors compétents puisque seul sera compétent le tribunal du centre principal des intérêts du demandeur. Toutefois, ce facteur peut être imprévisible à l'encontre de l'auteur du dommage.

Une autre solution, qui n'est pas en tant que telle un critère de rattachement, peut être mentionnée malgré l'imprévisibilité qui en émane : le forum « *non conveniens* ».

Le déclinement de compétence d'une juridiction au profit d'un autre tribunal plus compétent aux fins de trancher le litige, le forum « *non conveniens* » pourrait être appliqué à un litige relatif aux données personnelles .

Le « *forum non conveniens* » peut permettre d'éviter la pluralité de tribunaux saisis puisque le tribunal pourra choisir d'infirmer ou d'affirmer sa compétence au regard notamment de certains éléments mentionnés par la Cour du Québec dans l'arrêt Oppenheim forfait GMBH c. Lexus maritime inc.[232]

Sur internet, d'autres éléments pourraient être envisagés, telle que la langue utilisée sur le site internet, ou encore la langue de rédaction des commentaires des internautes.

Toutefois, le « *forum non conveniens* » présente un caractère d'imprévisibilité à l'égard de l'auteur du dommage. De plus, il convient de souligner encore une fois qu'il ne s'agit pas d'un critère de rattachement puisque ce n'est qu'une fois que le tribunal est saisi qu'une des parties au litige peut avoir recours au forum « *non conveniens* ».

Les autres solutions, le tribunal de l'État de localisation du serveur informatique, et le tribunal de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires ne sont tout simplement pas des solutions envisageables dans le cadre de l'attribution de la compétence juridictionnelle.

En matière de conflits de lois, trois solutions prévues par le droit commun se sont avérées être les plus intéressantes, voir même les meilleures : la loi de l'État du préjudice avec le respect de la condition de prévisibilité à l'égard de l'auteur du dommage, la loi de l'État du domicile du demandeur et du défendeur à l'instance, et la loi de l'État favorisant la victime.

La loi de l'État de survenance du préjudice est des plus intéressantes lorsque la condition de prévisibilité à l'égard de l'auteur du dommage est respectée. Il s'agit alors d'une solution juste tant à l'égard du demandeur qu'à l'égard du défendeur à l'instance.

Cependant, sur internet, la loi type de la CNUDCI[233] propose à chaque État de déterminer quelle disposition, parmi l'ensemble de dispositions, il mettra en place aux fins d'apprécier la

---

[232] *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).
[233] *Loi type de la CNUDCI sur le commerce électronique et guide pour son incorporation avec le nouvel article 5 bis tel qu'adopté en 1998,* Nations Unies, 1999, en ligne : < http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf > (consulté le 20 septembre 2015).

loi de réception de l'information. Or, en l'absence de détermination par les États de la disposition applicable, ce critère peut présenter un caractère incertain.

La loi de l'État du domicile du demandeur et du défendeur à l'instance est solution juste et équitable à l'égard de la victime et également de l'auteur du dommage.

La loi de l'État favorisant la victime est une solution profondément juste à l'égard de la victime d'une atteinte à son droit à la protection de ses données personnelles, et respecte le principe de prévisibilité envers l'auteur du dommage.

D'autres solutions relevant également du droit commun peuvent être mentionnées car elles sont intéressantes la loi de l'État où la faute a été commise et la loi de l'État de résidence du défendeur à l'instance.

La loi de l'État où la faute a été commise est prévisible envers le défendeur mais peut paraitre injuste à l'égard du demandeur à l'instance.

La loi de l'État de résidence du défendeur à l'instance respecte le principe de prévisibilité à l'encontre de l'auteur du dommage mais peut paraitre injuste à l'égard de la victime : le demandeur à l'instance pouvant choisir de commettre une faute dans son État de résidence en sachant que la loi de cet État ne sanctionne que très faiblement les atteintes au droit de la protection des données personnelles.

De la même manière, les critères du ciblage et de l'accessibilité s'appliquant à internet et envisagés par la doctrine, sont intéressants puisqu'ils permettent d'appuyer le choix de la loi de l'État de survenance de la faute ou du dommage par exemple.

Le ciblage peut permettre de conforter le choix de la loi de l'État de survenance du préjudice ou de commission de la faute. Il n'est pas possible d'avoir recours à ce facteur de rattachement de manière autonome dans la mesure où pris de façon individuel il est susceptible de présenter un caractère injuste à l'égard de la victime.

L'accessibilité est un critère intéressant en ce qu'il peut permettre de conforter l'application de la loi de l'État du dommage : c'est-à-dire que si le site est accessible par la victime dans l'État où elle prétend avoir subi le préjudice, alors ce sera la loi de cet État qui sera applicable et cela permettra d'éviter une multiplicité des lois applicables.

Enfin, certaines solutions ne sont absolument pas envisageables car trop imprévisibles et/ou injustes à l'égard de l'auteur ou de la victime du dommage : la loi de l'État du fournisseur d'accès à internet, de l'hébergeur et/ou des intermédiaires, la loi de l'État offrant la « *meilleure protection des données à caractère personnel* »,[234] et la loi de l'État où est établi le « *maître des fichiers* ».[235]

Pour conclure, nous allons choisir parmi l'ensemble des solutions identifiées, celles qui finalement semblent être les meilleures, c'est-à-dire celles respectant l'équité procédurale, la bonne administration de la justice, le principe de prévisibilité à l'égard du défendeur à l'instance, l'existence de liens suffisants entre le litige et le tribunal saisi, le principe de proximité et le principe de la détermination du centre des intérêts. Évidemment aucune des solutions étudiées ne respecte parfaitement l'ensemble de ces principes, mais il s'agit de choisir celles qui sont les plus respectueuses.

En matière de compétence juridictionnelle, la solution qui semble être la plus judicieuse hors et sur internet parait être le tribunal de l'État du domicile de la victime prévue en droit québécois.

En matière de conflits de lois, la solution la meilleure hors et sur internet est la loi de l'État du domicile ou de la résidence principale du demandeur et du défendeur à l'instance prévue par les droits québécois, européen et suisse, puisqu'elle est juste et équitable à l'égard des deux parties au litige. Toutefois, dans le cas où cette solution n'est pas envisageable car la situation ne présente pas d'éléments d'extranéité, la solution la meilleure est alors la loi de l'État favorisant la victime prévue par le droit suisse.

---

[234] BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992.
[235] *Id.*

Bibliographie

1. Traités et autres instruments internationaux, régionaux et nationaux

1.1. Instruments juridiques internationaux

- *Loi type de la CNUDCI sur le commerce électronique et guide pour son incorporation avec le nouvel article 5 bis tel qu'adopté en 1998,* Nations Unies, 1999, en ligne : <http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf> (consulté le 20 septembre 2015).
- *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, 1980, en ligne : <http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelavieprivееetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm> (consulté le 10 février 2015),

1.2. Instruments juridiques régionaux et/ou provinciaux

❖ **Europe**

- Communautés européennes, le Danemark, l'Islande, la Norvège et la Suisse, *Convention concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale*, 2007, en ligne : <https://www.admin.ch/opc/fr/classified-compilation/20082721/index.html> (consulté le 29 octobre 2015).

❖ **Québec**

- *Code civil du Québec,* L.Q., 1991, c. 64,
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* L.R.Q., c. A-2.1,
- *Loi sur la protection des renseignements personnels dans le secteur privé,* L.R.Q., c. P-39.1.

❖ **Union-Européenne**

➢ ***Traités***

- Conseil de l'Europe, *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales,* 1950, en ligne : <http://conventions.coe.int/Treaty/FR/Treaties/Html/005.htm> (consulté le 14 février 2015).
- CE, *Traité sur le fonctionnement de l'Union européenne (version consolidée),* 2012, en ligne : <http://eur-lex.europa.eu/legal content/FR/TXT/PDF/?uri=CELEX:12012E/TXT&from=FR> (consulté le 5 février 2015).
- Conseil européen, *Charte des droits fondamentaux de l'Union européenne,* 2000, en ligne : <http://www.europarl.europa.eu/charter/pdf/text_fr.pdf> (consulté le 13 février 2015),

➢ ***Règlements***

- CE, *Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)* (2012),
- CE, *Proposition de recommandations détaillées concernant le Règlement (CE) n°864/2007 sur la loi applicable aux obligations non contractuelles (Rome II) (2012).*
- CE, *Règlement (UE) n°1215/2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale,* 2012, en ligne : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:fr:PDF> (consulté le 27 février 2015).

- CE, *Règlement (CE) n. 864/2007 du Parlement européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (« Rome II »),* 2007, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32007R0864&from=FR> (consulté le 7 mars 2015),
- CE, *Règlement européen n.45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,* 2001, en ligne : <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:fr:PDF> (consulté le 7 février 2015).

➢ ***Directives***

- CE, *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* 1995, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR> (consulté le 15 février 2015).
- CE, *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),* 2002, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR> (consulté le 7 février 2015).

1.3. Instruments juridiques nationaux

❖ **États-Unis**

- The Senate and The House of representatives of the United States of America, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, H.R. 3162, 107ème, 1ère session, 5 (2001), en ligne: <http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf> (consulté le 11 février 2015).

❖ **France**

- *Code civil.*

❖ **Suisse**

- *Loi fédérale sur le droit international privé,* 18 décembre 1987, 291.
- *Loi fédérale sur la protection des données*, 19 juin 1992, 235.1.
- *Constitution fédérale de la Confédération suisse*, 18 avril 1999, 101.

2. Jurisprudence

2.1. Jurisprudence États-Unis

- *Babcock v. Jackson*, 191 N.E.2d 279 (N.Y. 1963).

2.2. Jurisprudence française

- Crim., 14 mars 2006, *Bull. crim.,* n.69.
- Civ.1ère, 13 avril 1988, *Bull.civ.*, n°98.

2.3. Jurisprudence québécoise

- *Maria Pia Grillo c. Google inc.,* C.Q. Montréal (Ch. Civ.), n. 500-32-130991-112, 3 octobre 2014, en ligne : <http://fr.scribd.com/doc/244927017/Google-Street-View-Case#scribd> (consulté le 3 mars 2015),
- *Facebook inc. c. Guerbez*, C.S.Q. Montréal, n. 500-17-053752-096, 28 septembre 2010, en ligne : <http://fr.scribd.com/doc/38806669/Quebec-Superior-Court-judgment-against-Adam-Guerbuez#scribd> (consulté le 20 avril 2015),

- *National Bank of Canada c. Weir,* [2010] R.J.Q. 823 (C.S),
- *Investor group c. Hudson,* [1999] R.J.Q. 599 (C.S),
- *Aubry c. Éditions Vice-Versa,* [1998] 1 R.C.S 591,
- *Oppenheim forfait GMBH c. Lexus maritime inc.*, 1998 CanLII 13001 (QC C.A.).

2.4. Jurisprudence suisse

- Cour de Justice de Genève, 19 juin 2009, ACJC/790/09.

2.5. Jurisprudence Union européenne

- *K.U c. Finlande,* n° 2872/02, CEDH 2008.
- *Maximillian Schrems c. Data Protection Commissioner,* Affaire C-362/14, 6 octobre 2015, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=50254>, (consulté le 20 octobre 2015);
- *eDate Advertising GmbH c. Olivier Martinez,* Affaire C-509/09 et -161/10, 25 octobre 2011, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=95492> (consulté le 6 avril 2015),
- *Hôtel Apenhof c. Oliver Heller,* Affaire C-144/09, 7 décembre 2010, en ligne : <http://curia.europa.eu/juris/document/document.jsf?text=&docid=83437&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=96720> (consulté le 7 avril 2015),
- *Fiona Schevill c. Presse Alliance SA.*, Affaire C-68/93, CJCE, 7 mars 1995, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:61993CJ0068&from=FR> (consulté le 27 février 2015).

- *Handelskwekerig G.J. Bier BV c. Mines de Potasse d'Alsace SA.,* Affaire C-21/76, CJCE, 30 novembre 1976, en ligne : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:61976CJ0021&from=FR> (consulté le 20 septembre 2015).

3. Doctrine

3.1. Monographies

- BENYEKHEL, K., *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, éd. Thémis, 1992, 475p.,
- GOLDSTEIN, G., *Commentaires sur le Code civil du Québec, Droit international privé, vol. 2, Compétence internationale des autorités québécoises et effets des décisions étrangères (art. 3134 à 3168 C.c.Q.)*, éd. Yvon Blais, 2013, n° 3135-500 à 3135-590,
- GOLDSTEIN, G., GROFFIER, E., *Droit international privé: Tome II règles spécifiques,* Cowansville, Québec, éd. Yvon Blais, 2003, 1253p.,
- GOLDSTEIN, G., GROFFIER, E., *Traité de droit civil. Droit international privé*, vol. 1, *Théorie générale*, Cowansville, éd. Yvon Blais, 1998, n° 134,
- GOLDSTEIN, G., *De l'exception d'ordre public aux règles d'application nécessaire: Étude du rattachement substantiel impératif en droit international privé canadien,* Montréal, éd. Thémis, 1996, 647p.,
- EMANUELLI, C., *Droit international privé québécois*, 3ème éd. Wilson & Lafleur, 2011, n° 164-167,
- HUET, J., DREYER, E., *Droit de la communication numérique*, coll. "Manuel", Paris, éd. LG.D.J Lextenso, 2011, 376p.,
- MAYER, P., HEUZÉ, V., *Droit international privé,* coll. Domat droit privé, 9ème éd., Paris, éd. Montchrestien, 2007, 798p.,
- OCDE, *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris, éd. Organisation de coopération et de développement économiques, 2002, 72p.,

- TALPIS, J.A., et CASTEL, J.-G, «Le Code civil du Québec — Interprétation des règles de droit privé» dans *La Réforme du Code civil*, t. 3, Québec, Presses de l'Université Laval, 1993, 902, n° 411 et s.,
- TURK, A., *La vie privée en péril : Des citoyens sous contrôle*, coll. « OJ.SC. Humaines », Paris, éd. Odile Jacob Broché, 2011, 272 p.

3.2. Chapitres de livres

- BENYEKHLEF, K., « Les normes internationales de protection des données personnelles et l'autoroute de l'information » dans *La vie privée dans l'entreprise*, Thémis, Montréal, Actes des Journées Maximilien-Caron, éd. Thémis, 1996, p. 65,
- GLENN, H.P., «Droit international privé», dans *La réforme du Code civil*, Barreau du Québec et Chambre des Notaires du Québec, P.U.L., Sainte-Foy, 1993, 669, n° 73,
- GOLDSTEIN, G., «Chap. Canada (Québec)», *in Declining Jurisdiction in Private International Law*, par J.J. Fawcett (éd.), Oxford, Clarendon Press, 1995, 146-157,
- LEBEL, L., et CHABOT, G., «L'essai d'un mariage : l'intégration du forum non conveniens dans le droit international privé québécois», dans *Mélanges en l'honneur du professeur Alain Prijuner,* par S. Guillemard (dir.), Thomson Reuters Canada, 2011., 267,
- SABOURIN, F., «Motifs permettant de ne pas exercer la compétence : *forum non conveniens* et litispendance internationale», fascicule 9, dans *JurisClasseur Québec*, volume *Droit international privé*, LexisNexis, feuilles mobiles,
- SAUMIER, G., «Le *forum non conveniens* au Québec: bilan d'une transplantation», dans *Mélanges en l'honneur du professeur Alain Prijuner*, par S. Guillemard (dir.), Thomson Reuters Canada, 2011, 345,

3.3. Articles de revues

- CASTEL, M., «Jurisdiction and Choice of Law Issues in Multistate Defamation on the internet», (2013) 51 *Alberta Law Review* 153,
- DUPUIS, M., « La vie privée à l'épreuve des réseaux sociaux », (2013) 102 *Revue Lamy Droit civil* 39,
- GUILLEMARD, S., PRUJINER, A., SABOURIN, F., « Les difficultés de l'introduction du *forum non conveniens* en droit québécois », (1995) 36 *C. de D.* 91.,

- GUILLEMARD, S., et TÊTE, M., « Le forum non conveniens au Québec, une vingtaine d'années plus tard : encore quelques questions non résolues », (2012) 25.1 *Revue québécoise de droit international* 175.
- HALPÉRIN, J.-L., « Diffamation, vie publique et vie privée en France de 1789 à 1944 », (2013) 65 *Droit et cultures* 145,
- LALIVE AVOCATS, « Chronique de jurisprudence suisse, loi fédérale de droit international privé (LDIP) du 18 décembre 1987 (2005-2009) », (2011) 2 *Journal du droit international* 465.
- MORRIS, J.H.C., « The proper law of a tort », (1951) 64 *Harvard Law Review* 881,
- SAUMIER, G., «*Forum non conveniens*, Where are we now?», (2000) 12 *S.C.L.R.* (2d) 121,
- TALPIS, J.A, et KATH, S. L., «The Exceptional as Commonplace in Quebec *Forum non conveniens* Law: *Cambior*, a case in Point», (2000) 34 *R.J.T.* 761,
- TREMBLAY, M., « Flux transfrontalières de données et protection de la vie privée », (2010) vol. III *Cahier de recherches,*

3.4. Rapports et communiqués

- ALVERGNAT, C., CNIL, *Rapport sur le publipostage électronique et la protection des données personnelles*, Paris, 1999, <http://www.diocese-alsace.fr/docs/juridiques/loi-cnil-publipostage.pdf> (8 janvier 2015),
- Comité des Ministres, Conseil de l'Europe, *Convention sur la cybercriminalité Rapport explicatif*, Budapest, 2001, en ligne : <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_explanatoryreport_/7_explanatoryreport_fr.pdf> (consulté le 5 février 2015),
- FAUCHON, P., *Communication de la République Hellénique: initiative de la République hellénique concernant l'adoption par le Conseil d'un projet de décision-cadre relative à l'application du principe non bis in idem*, Paris, 2003, en ligne : <http://www.senat.fr/ue/pac/E2236.html> (consulté le 4 février 2015),

- GOSSELIN, P., Assemblée nationale, *Rapport fait au nom de la Commission des affaires européennes sur la proposition de résolution européenne (n.4227) de M. Philippe Gosselin sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Paris, 2012,
- PARLEMENT EUROPÉEN, *Rapport contenant des recommandations à la Commission sur la modification du règlement (CE) n°864/2007 sur la loi applicable aux obligations non contractuelles (Rome II),* Bruxelles, 2 mai 2012, en ligne : <http://www.alain-bensoussan.com/wp-content/uploads/22798084.pdf> (consulté le 14 mars 2015),
- TRUDEL, P., AUBRAN, F., DUPUIS, G., Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Montréal, 2007, p.7.
- WALTER, J-P., Conseil de l'Europe, *Défis posés par les flux transfrontières de données à caractère personnel,* Madrid, p.2.

3.5. Articles de journaux

- CHEMINAT, J., « Un pas de plus vers le règlement européen sur la protection des données privées », *lemondeinformatique* (12 mars 2014), en ligne : <http://www.lemondeinformatique.fr/actualites/lire-un-pas-de-plus-vers-le-reglement-europeen-sur-la-protection-des-donnees-privees-56841.html> (consulté le 3 mars 2015),
- ESTIENNE, Y., «Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposés», *Communication Le Creis* (2010), en ligne : <http://www.lecreis.org/colloques%20creis/2010/Communication-Estienne-CREIS.pdf> (consulté le 2 avril 2015),
- FANEN, S., «La notion d'auteur doit être remise en cause», *Libération écrans* (2012), en ligne : <http://ecrans.liberation.fr/ecrans/2012/11/30/la-notion-d-auteur-doit-etre-remise-en-cause_949274> (consulté le 3 mai 2015),

- LAMBERT-CHAN, M., «Les médias sociaux décuplent les poursuites pour diffamation», *UdeMNouvelles*, 9 mai 2011, en ligne : <http://www.nouvelles.umontreal.ca/recherche/sciences-sociales-psychologie/20110509-les-medias-sociaux-decuplent-les-poursuites-pour-diffamation.html> (consulté le 2 novembre 2015),
- OBS Monde, «Qu'est-ce que le Patriot Act», *L'obs Monde* (6 septembre 2006), en ligne : <http://tempsreel.nouvelobs.com/monde/20060906.OBS0822/qu-est-ce-que-le-patriot-act.html> (consulté le 29 avril 2015),
- PIXELS, « Interdiction des photos de nu: la justice confirme que Facebook peut être jugé en France», *Le Monde* (2015), en ligne : <http://www.lemonde.fr/pixels/article/2015/03/05/la-justice-confirme-que-facebook-peut-etre-juge-en-france_4588376_4408996.html> (consulté le 1 mai 2015),
- PIXELS, « Tim Cook estime que les États-Unis sont allés trop loin dans la collecte des données », *Le Monde* (2014), en ligne : <http://www.lemonde.fr/pixels/breve/2014/09/16/tim-cook-estime-que-les-etats-unis-sont-alles-trop-loin-dans-la-collecte-des-donnees_4488172_4408996.html> (consulté le 20 novembre 2014),
- SLOIM, E., « Pourquoi l'accessibilité numérique? », *Openweb* (25 juillet 2005), en ligne : <http://openweb.eu.org/articles/accessibilite_numerique_pourqu> (consulté le 11 avril 2015).

4. Autres

4.1. Notes de cours

- TRUDEL, P., *Notes du cours* DRT 3805 (*Droit des technologies de l'information*), Montréal, en ligne : <http://www.chairelrwilson.ca/cours/drt3805g/reputation.pdf>, (consulté le 6 mars 2015),
- TRUDEL, P., *Notes du cours* DRT 3805G (*Droit des technologies de l'information*), Montréal, en ligne : <http://www.chairelrwilson.ca/cours/drt3805g/image.html> (consulté le 6 mars 2015),

- TRUDEL, P., *Notes du cours* DRT 3805G (*Droit des technologies de l'information*), Montréal, en ligne : <http://www.chairelrwilson.ca/cours/drt3805g/rebeiro.html> (consulté le 6 mars 2015).

4.2. Thèse ou mémoire

- SINOPOLI, L., *Le procès équitable dans les rapports privés internationaux – Recherche sur le champ d'application de l'article 6 paragraphe 1re de la Convention européenne des droits de l'homme en droit international privé*, Thèse, Paris, Université Paris 1 Panthéon-Sorbonne, 2000.

4.3. Sites internet

- Administration française, « Droit à l'image et protection de la vie privée », *service public* (22 mai 2014), en ligne : <http://vosdroits.service-public.fr/particuliers/F32103.xhtml> (consulté le 6 avril 2015),
- BRAUDO, S., « Définition de Domicile, domiciliation », dictionnaire du droit privé, en ligne : <http://www.dictionnaire-juridique.com/definition/domicile-domiciliation.php>, (consulté le 23 septembre 2015).
- Commissariat à la protection de la vie privée du Canada, « Lois sur la protection des renseignements personnels au Canada », (15 mai 2014), en ligne : <https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_f.asp> (consulté le 4 avril 2015),
- Commission de la protection de la vie privée, « Questions les plus fréquemment posées - Flux transfrontières de données à caractère personnel », *privacycommission,* en ligne : <https://www.privacycommission.be/fr/faq-page/374#t374n7382> (consulté le 2 avril 2015),
- Commission nationale de l'informatique et des libertés, « Cookies & traceurs : que dit la loi? », *CNIL*, en ligne : <http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/ > (consulté le 14 février 2015),

- Commission nationale de l'informatique et des libertés, « La directive 2006/24/CE contraire aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne », *CNIL* (18 avril 2014), en ligne : <http://www.cnil.fr/linstitution/actualite/article/article/la-directive-200624ce-contraire-aux-articles-7-et-8-de-la-charte-des-droits-fondamentaux-de-lun/> (site consulté le 5 février 2015),
- Commission Nationale de l'Informatique et des Libertés, « Safe Harbour », *CNIL,* en ligne : <http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/safe-harbor/> (consulté le 23 septembre 2015),
- Centre national de la recherche scientifique, « Loi informatique et libertés », *cnrs,* en ligne : <http://www.cil.cnrs.fr/CIL/spip.php?rubrique281> (consulté le 20 mai 2015)
- Conseil de l'Europe, « Agir contre la criminalité économique », *coe.int,* en ligne : <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp> (consulté le 10 mai 2015),
- Dictionnaire de la High Tech, « Spyware logiciel espion », en ligne : <http://encyclopedie.linternaute.com/definition/491/5/spyware.shtml> (consulté le 10 février 2015),
- Europa, « La directive », (1re septembre 2010), en ligne : <http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l14527_fr.htm> (consulté le 17 février 2015),
- Europa, « Le règlement », (12 août 2010), en ligne : <http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l14522_fr.htm> (consulté le 17 février 2015),
- Europa, « Protection des données à caractère personnel », (1 février 2011), en ligne : <http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm> (consulté le 5 février 2015),

- Europe, « Protection des données dans le secteur électronique », (19 mai 2010), en ligne : <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_fr.htm> (consulté le 2 avril 2015),
- Gendarmerie Royal du Canada, « Courriels frauduleux et hameçonnage (phishing) », (29 janvier 2015), en ligne : <http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-fra.htm> (consulté le 10 février 2015),
- Gouvernement Canada Ministère de la Justice, « Fiche terminologique bijuridique », *justice.gc.ca* (7 janvier 2015), en ligne : <http://www.justice.gc.ca/fra/sjc-csj/harmonization/bijurilex/terminolog/not176.html> (consulté le 13 avril 2015),
- Lexis Nexis, « Qualification en droit international privé », Lexisnexis.fr, en ligne : <http://www.lexisnexis.fr/droit-document/fascicules/jcl-droit-international/126_EG_DI0_510126CH_1_PRO_231696.htm#.VgaspiDtmkq> (consulté le 2 septembre 2015),
- Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, « Le cyber-harcèlement », *agir contre le harcèlement à l'école.gouv.fr*, en ligne : <http://www.agircontreleharcelementalecole.gouv.fr/quest-ce-que-le-harcelement/le-cyberharcelement/> (consulté le 9 février 2015),
- Parlement européen Actualités, « Des règles plus strictes pour protéger les données personnelles à l'ère du numérique », (12 mars 2014), en ligne : <http://www.europarl.europa.eu/news/fr/news-room/content/20140307IPR38204/html/Des-r%C3%A8gles-plus-strictes-pour-prot%C3%A9ger-la-vie-priv%C3%A9e-%C3%A0-l'%C3%A8re-num%C3%A9rique> (consulté le 3 mars 2015),
- République française, « Chaque citoyen a-t-il droit au respect de sa vie privée ? », *vie publique* (9 octobre 2013), en ligne :

<http://www.vie-publique.fr/decouverte-institutions/citoyen/citoyennete/definition/droits/chaque-citoyen-t-il-droit-au-respect-vie-privee.html> (consulté le 20 avril 2015),

- The Canadian Bar association British Columbia Branch, « Defamation : Libel and Slander », *cbabc* (mars 20140, en ligne : <http://cbabc.org/For-the-Public/Dial-A-Law/Scripts/Your-Rights/240> (consulté le 4 mars 2015),
- Toute l'Europe, « La protection des données personnelles en Europe », *Toutel'Europe.eu* (10 juin 2014), en ligne : <http://www.touteleurope.eu/actualite/la-protection-des-droits-fondamentaux-donnees-privees-droit-a-l-oubli.html> (consulté le 3 avril 2015),
- Wikipédia Encyclopédie libre, « La convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe », *Wikipédia* (15 mars 2013), en ligne : <http://fr.wikipedia.org/wiki/Convention_pour_la_protection_des_personnes_%C3%A0_l%27%C3%A9gard_du_traitement_automatis%C3%A9_des_donn%C3%A9es_%C3%A0_caract%C3%A8re_personnel> (consulté le 21 mai 2015),
- Wikipédia Encyclopédie libre, « Tor (réseau) », *Wikipédia* (23 avril 2015), en ligne : <http://fr.wikipedia.org/wiki/Tor_%28r%C3%A9seau%29> (consulté le 10 mai 2015).

4.3. Autres

- POITRAS, L., « Citizenfour », *plateforme en ligne youtube.com* (2014), en ligne : <https://www.youtube.com/watch?v=L8ygeb6F8ww> (consulté le 4 mai 2015),
- VALENTIN, A., « Un œil sur la planète – Citoyens sous surveillance ! », *arte.documentaire* (2015), en ligne : <https://www.youtube.com/watch?v=oGk-9wIwWUQ> (consulté le 5 mai 2015).